ISTRUZIONI PER LA SEGNALAZIONE DEI GRAVI INCIDENTI OPERATIVI O DI SICUREZZA[1] – SIGNIFICANT INSTITUTION ITALIANE E BANCHE AUTORIZZATE IN ITALIA APPARTENENTI A SIGNIFICANT INSTITUTION STRANIERE

Il presente documento contiene le istruzioni per effettuare la valutazione di gravità di un incidente operativo o di sicurezza ai fini della segnalazione alla Banca d'Italia e per l'invio della segnalazione stessa. La Banca d'Italia inoltra alla Banca centrale europea e/o all'Autorità bancaria europea i rapporti ricevuti laddove previsto dalla procedura di segnalazione riguardante gli incidenti cyber definita a livello SSM e dalla procedura di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2).

Indice

1.	**Definizioni**	**1**
2.	**Modalità di segnalazione**	**3**
3.	**Criteri e soglie per la segnalazione**	**6**
4.	**Il modello per la segnalazione degli incidenti operativi o di sicurezza**	**13**
ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione		29

1. Definizioni

1.1. Ai sensi della Circ. n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, Tit. IV, Cap. 4, Sez. 1, Par. 3), con "incidente operativo o di sicurezza" si intende "ogni evento, o serie di eventi collegati, non pianificati dalla banca 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)";

1.2. 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

[1] Fino al 34° Aggiornamento della Circolare n.285, altrimenti definito "incidente di sicurezza informatica".

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)).

1.3. Tali eventi includono, a titolo di esempio:

- 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;
- 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, 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.

Nel seguito del documento e ai fini del framework in oggetto, gli incidenti operativi o di sicurezza vengono classificati come:

- Incidenti 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 banca o incidenti che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario.
- Incidenti operativi: 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.

Di seguito infine alcune definizioni di termini adottati nel documento:

- Integrità: Proprietà della salvaguardia dell'esattezza e completezza delle risorse (inclusi i dati).
- Disponibilità: Proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento.

- Riservatezza: Proprietà per cui le informazioni non sono rese disponibili o divulgate a persone, entità o procedure non autorizzate.
- Autenticità: Proprietà di una fonte di essere quella che dichiara di essere.
- Servizi connessi ai pagamenti: Attività commerciali definite nell'articolo 4, paragrafo 3, della PSD2 e tutte le attività di supporto tecnico necessarie per la corretta fornitura dei servizi di pagamento.

2. Modalità di segnalazione

La capogruppo segnala su base consolidata tutti gli incidenti gravi, operativi[2] o di sicurezza a prescindere dal fatto che si verifichino presso succursali o affiliate all'interno o al di fuori dell'area dell'euro[3].

Per ogni incidente la segnalazione consta di tre tipologie di rapporti:

- **First Report:** il primo report relativo all'incidente, atteso entro due ore dal momento in cui esso è stato classificato come "grave" secondo i criteri descritti nella sezione 3.

  L'intermediario classifica l'incidente in modo tempestivo dopo che l'incidente è stato rilevato, ma non oltre 24 ore dopo la rilevazione dell'incidente, e senza indebito ritardo dopo che le informazioni necessarie per la classificazione dell'incidente diventano disponibili. Se è necessario più tempo per classificare l'incidente, gli intermediari ne spiegano i motivi nell'apposito campo del primo report.

  L'intermediario include nel primo report le informazioni basilari (ossia quelle di cui alla sezione in rosso del modulo), indicando alcune caratteristiche fondamentali dell'incidente e le sue conseguenze previste sulla base delle informazioni disponibili subito dopo che è stato rilevato e classificato. L'intermediario ricorre a stime quando non sono disponibili i dati effettivi.

  L'incidente grave va segnalato anche se è stato risolto prima della sua classificazione.

  Una volta ricevuta la segnalazione, la Banca d'Italia comunicherà all'intermediario un codice di riferimento (*Incident ID*) che identifica univocamente l'incidente. L'intermediario deve indicare nell'apposito campo del modulo questo codice di riferimento quando trasmette i successivi report oppure un aggiornamento del primo report.

[2] In linea con gli Orientamenti EBA, le banche applicano le disposizioni per la gestione degli incidenti operativi o di sicurezza alla gestione degli incidenti operativi relativi alla prestazione dei servizi di pagamento anche se non collegati al funzionamento delle risorse e dei processi ICT.

[3] Le istruzioni si applicano anche se il grave incidente operativo o di sicurezza ha origine al di fuori dell'dell'Italia (ad esempio, quando un incidente ha origine presso la società capogruppo o una succursale costituita al di fuori dell'Italia) e riguarda i servizi di pagamento forniti da un prestatore di servizi di pagamento con sede in Italia direttamente (un servizio connesso ai pagamenti è effettuato dalla società colpita costituita al di fuori dell'Italia) o indirettamente (la capacità del prestatore di servizi di pagamento di continuare a svolgere l'attività di pagamento viene compromessa in qualche altro modo a causa dell'incidente).

- **Interim Report:** il report ad interim, inviato quando le regolari operazioni sono state ripristinate e l'attività è tornata alla normalità (chiusura dell'incidente[4]). Se le normali attività non sono state ancora ripristinate, il report va trasmesso comunque entro tre giorni lavorativi dalla trasmissione del primo report.

  Successivamente, per tutta la durata dell'incidente, l'intermediario sottomette un ulteriore report ad interim ogniqualvolta venga a conoscenza di cambiamenti significativi rispetto al rapporto precedente (ad esempio, se la gravità dell'incidente aumenta o diminuisce, se sono state identificate nuove cause o intraprese azioni per risolvere il problema, se l'incidente viene risolto dopo tre giorni lavorativi dalla trasmissione del rapporto iniziale).

  L'intermediario sottomette il report ad interim con una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione in blu del modulo). Inoltre, l'intermediario fornisce gli eventuali ulteriori report ad interim aggiornando le informazioni già inserite nelle sezioni rossa e blu del modulo. In ogni caso, l'intermediario presenta un report ad interim quando esplicitamente richiesto dalla Banca d'Italia.

  Come nel caso del primo report, qualora dati effettivi non siano disponibili, l'intermediario può ricorrere a stime.

  Se l'attività dovesse ritornare alla normalità prima che siano trascorse due ore dalla classificazione dell'incidente "grave", l'intermediario deve adoperarsi per presentare simultaneamente sia il primo report sia il report ad interim (ossia compilando le sezioni rossa e blu del modulo) entro le due ore previste per l'invio del primo report.
- **Final Report:** il report finale, inviato entro 20 giorni lavorativi dalla chiusura dell'incidente (momento in cui si considera che le attività siano tornate alla normalità).

  Il report finale deve essere inviato una volta effettuata 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. Nel report finale devono essere compilati i campi in verde. Laddove l'intermediario necessiti di una proroga del termine di 20 giorni lavorativi (ad esempio, se non sono ancora disponibili dati effettivi sull'impatto o le cause all'origine dell'incidente non siano state ancora individuate), questi deve contattare la Banca d'Italia prima della scadenza di suddetto termine e fornire una giustificazione adeguata per il ritardo e una nuova data stimata per il report finale.

  Nel caso di chiusura del grave incidente entro le due ore dal momento della sua classificazione, laddove l'intermediario sia in grado di fornire tutte le informazioni richieste dal rapporto intermedio

[4] La normale attività è da considerare ristabilita quando le attività/operazioni sono state ripristinate allo stesso livello di servizio/alle stesse condizioni definiti dall'intermediario o disposti esternamente da un accordo sul livello dei servizi (SLA), in termini di tempi di elaborazione, capacità, requisiti di sicurezza, ecc., e le misure di emergenza non sono più in vigore.

e dal rapporto finale, esso dovrebbe adoperarsi per fornire congiuntamente le informazioni relative al rapporto iniziale, intermedio e finale (ossia compilare le sezioni rossa, blu e verde del modulo).

Nel caso il report finale non includa tutte le informazioni necessarie perché non disponibili nei tempi richiesti (venti giorni lavorativi dalla chiusura dell'incidente), all'intermediario sarà richiesto di inviare una relazione di chiusura, eventualmente nel formato standard del report finale o libero a seconda dei casi.

L'intermediario deve inviare inoltre un report finale nel momento in cui, ad esito delle analisi sull'incidente svolta nel continuo, ritenga che un incidente già segnalato non soddisfi più i criteri per essere considerato grave e non si prevede che li soddisferà prima che l'incidente sia chiuso. In tale eventualità, l'intermediario deve inviare il report finale non appena questa circostanza viene rilevata e, in ogni caso, entro la scadenza per la trasmissione del report successivo. In questa particolare situazione, invece di compilare i campi in verde del modulo, l'intermediario deve selezionare la casella "Incident reclassified as non-significant" e fornire una spiegazione dei motivi che giustificano questa riclassificazione.

Il modulo da utilizzare per i suddetti report è annesso alle presenti istruzioni (cfr. documento "comunicazione_incidenti_SI_2021.pdf"). Gli intermediari, laddove ritenuto necessario, possono integrare il modulo standardizzato con ulteriore documentazione, sotto forma di uno o più allegati. Per la compilazione dei campi presenti nel modulo, gli intermediari seguono le istruzioni contenute nel presente documento.

L'intermediario invia il modulo di segnalazione dell'incidente e gli eventuali documenti allegati in forma cifrata nel caso di incidente cyber laddove la rivelazione di informazioni contenute nel modulo potrebbe avere significativi impatti negativi sull'intermediario o altri soggetti coinvolti. Per cifrare il modulo l'intermediario deve utilizzare <u>tutte</u> le chiavi di crittografia annesse alle presenti istruzioni (bdi_key1.p7b, bdi_key2.p7b, bdi_key3.p7b, bdi_key4.p7b)[5].

Gli intermediari devono, in ogni momento, preservare la riservatezza e l'integrità delle informazioni trasmesse.

Ogni rapporto (eventualmente in forma cifrata) dovrà essere allegato ad un messaggio di posta elettronica certificata e inviato alla casella di PEC Supervisione_rischio_ICT@pec.bancaditalia.it; l'oggetto del messaggio dovrà indicare il rapporto allegato, il tipo di incidente segnalato e l'ente segnalante, secondo il seguente schema: "Oggetto: Com_incidente WWWW ZZZZ – XXXXX YYYYY", dove WWWW va valorizzato con "PRIMO", "INTERIM", "FINALE", "RELAZIONE" (nel caso di relazione successiva al rapporto finale) con riguardo al rapporto allegato, ZZZZ con "CYBER" o "ALTRO" a seconda del tipo di

[5] Allo scopo di cifrare il documento con i certificati forniti è necessario che l'applicazione di crittografia utilizzata dall'intermediario sia compatibile con il protocollo PKCS #7.

incidente segnalato, mentre XXXXX e YYYYY rappresentano rispettivamente il codice ABI e il nome della banca segnalante.

Nel caso non sia possibile inviare la comunicazione in forma elettronica (ad esempio per l'impossibilità ad utilizzare la PEC a causa dello stesso incidente) l'intermediario comunica l'evento per via telefonica alla Divisione di analisi di vigilanza della Banca d'Italia di competenza.

Altre comunicazioni sul tema alla Banca d'Italia, non contenenti i moduli o informazioni relative all'incidente ma ad esempio richieste di chiarimenti o relative a proroghe dei termini di invio, devono essere inviate alla casella di posta elettronica SSI_incidenti@bancaditalia.it.

La Banca d'Italia informerà l'intermediario nel caso di inoltro dei report alla Banca centrale europea e/o all'Autorità bancaria europea.

Gli intermediari devono inoltre presentare alla Banca d'Italia, quando l'incidente ha interessato servizi di pagamento, una copia delle comunicazioni che sono state effettuate (o saranno effettuate) ai propri clienti, come previsto dall'articolo 96, paragrafo 1, comma 2, della PSD2, non appena disponibili.

Gli intermediari devono, su richiesta della Banca d'Italia, fornire qualsiasi documento supplementare che integri le informazioni trasmesse con il modulo ovvero rispondere a tutte le richieste di fornire ulteriori informazioni o chiarimenti riguardanti la documentazione già presentata

Al fine di chiarire il processo di segnalazione nei differenti casi, nell'Allegato 1 si riporta una descrizione grafica di possibili scenari di segnalazione.

3. Criteri e soglie per la segnalazione

Al verificarsi di un incidente operativo o di sicurezza, l'intermediario ne valuta la rilevanza utilizzando i criteri di seguito specificati e lo classifica conseguentemente come "grave" o "non grave" ai fini della segnalazione.

Per quanto riguarda le soglie "qualitative" (criteri a), c), d), e), i)), perché un incidente sia classificato come "grave" è sufficiente che uno solo dei criteri indicati sia soddisfatto per almeno un'entità del gruppo.

Per quanto riguarda le soglie "quantitative" (criteri b) ,f), g), h)), tali soglie devono essere considerate a livello consolidato se l'incidente riguarda il gruppo nel suo insieme, o a livello individuale delle singole entità colpite se l'incidente interessa una o più entità del gruppo[6].

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 l'intermediario.

[6] A titolo di esempio, se l'incidente interessa i sistemi informativi della capogruppo che forniscono servizi a tutte o parte delle entità del gruppo, tale incidente si considera "di gruppo". Se l'incidente interessa i sistemi informativi di una singola entità, tale incidente e i criteri di classificazione vanno considerati riferiti alla sola entità colpita.

Infatti, l'attenzione da parte dei media indica che la stampa e probabilmente i cittadini considerano l'incidente abbastanza rilevante da essere divulgato. Inoltre la comunicazione pubblica di un incidente operativo o di sicurezza può minare la fiducia nell'intermediario.

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, ciò potrebbe accadere 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 (e.g. Chief Information Officer or equivalent) (*Alto livello di escalation interna (es. CIO o equivalente)*)

La gestione dell'incidente è soggetta ad un'escalation[7] che lo porta, internamente, all'attenzione del responsabile aziendale per la funzione informatica (Chief Information Officer), ovvero di un livello manageriale equivalente o superiore, per assumere delle decisioni sull'incidente, al di fuori del processo ordinario/periodico di relazione sugli incidenti operativi o di sicurezza registrati.

Ad esempio, in genere il responsabile aziendale per la sicurezza informatica (*Chief Information Security Officer*, CISO) discute degli incidenti di sicurezza con il proprio staff quotidianamente, mentre la posizione di livello superiore (ossia il CIO) viene informata soltanto degli incidenti che richiedono un'azione più ampia o possono avere un impatto grave. In questo caso, il ricorso al CIO nella procedura di *escalation* di un incidente significherebbe che quest'ultimo è da ritenersi "grave".

Diversa è la situazione in cui, laddove il CIO discute di incidenti di sicurezza con frequenza giornaliera o settimanale, l'incidente sia portato alla sua attenzione soltanto nell'ambito di tale processo ordinario, insieme ad eventuali altri incidenti occorsi; in questo caso, non essendo interessate dall'escalation dell'incidente né il CIO né altre figure aziendali di livello manageriale pari o superiore, l'incidente è da considerarsi "non grave".

Dal momento peraltro che le figure professionali e i processi di gestione variano da intermediario a intermediario, ciascuno potrà valutare quale sia il livello manageriale più opportuno da considerare, ove sia interessato dalla procedura di *escalation*, quale segnale della gravità di un incidente.

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 l'intermediario in un numero elevato di azioni legali va classificato come "grave".

[7] L'"escalation" è la conduzione della gestione di un incidente caratterizzata da un aumento progressivo dei livelli aziendali coinvolti, fino a giungere, ove necessario, all'organo di amministrazione (cfr Circ. 285 - Parte Prima - Tit. IV - cap.5 - Allegato A).

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[8]) e/o l'attivazione del "CODISE (continuità di servizio)" per il coordinamento delle crisi operative della piazza finanziaria italiana.

Un BCP contiene diverse procedure che possono essere innescate da un incidente operativo o di sicurezza, tra cui:

- l'attivazione del piano di disaster recovery (disaster recovery plan, DRP);
- comunicazioni di emergenza e allerta dei membri dei team addetti al disaster recovery e di altri soggetti coinvolti;
- le procedure di backup e ripristino (in formato cartaceo ed elettronico) dei dati;
- il 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;
- valutazioni finanziarie e operative al fine di identificare cambiamenti nell'esposizione al rischio operativo, finanziario e creditizio a seguito di un incidente;
- processi di segnalazione regolamentare avviati dopo un incidente allo scopo di garantire il costante rispetto degli obblighi di segnalazione regolamentare;
- 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 una polizza contro i rischi informatici (cyber insurance) per coprire le perdite finanziarie derivanti dall'incidente.

Una *cyber insurance* è un prodotto assicurativo che protegge l'azienda contro i rischi informatici e, più in generale, contro i rischi connessi alle infrastrutture e alle attività informatiche. Le prestazioni offerte da tali piani assicurativi possono includere la copertura del contraente contro perdite come la distruzione di dati, l'estorsione, il furto, gli attacchi di pirateria informatica o di negazione di servizio; la copertura di responsabilità per il risarcimento di aziende a fronte di danni a terzi causati, tra le altre cose, da errori e omissioni, mancata protezione dei dati o diffamazione;

[8] Con "piano di continuità operativa" (o business continuity plan, BCP) si intende il documento che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse, per la gestione della continuità operativa dei processi aziendali critici e a rilevanza sistemica. Il BCP integra il piano di ripristino da disastro (o disaster recovery plan, DRP), finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. Cfr. Circ. 285 – Titolo IV – Capitolo 5.

altri benefit quali audit di sicurezza regolari, spese di comunicazione e d'indagine successive all'incidente e fondi per la ricompensa di chi fornisce informazioni sui responsabili.

C) L'incidente operativo o di sicurezza attiva o potrebbe attivare altre procedure di gestione delle crisi.

Procedure interne di gestione delle crisi che vengono avviate per gestire/mitigare l'incidente (a livello di gruppo).

A seconda dell'impostazione dei processi interni e/o della struttura dell'organizzazione informatica dell'intermediario, è possibile adottare diverse misure in risposta a un incidente come:

- attivare piani di emergenza;
- convocare il team/l'unità di gestione delle crisi dell'intermediario;
- convocare il comitato di crisi;
- convocare il comitato per la sicurezza informatica;
- coinvolgere nella procedura di *escalation* i team di livello basso/medio/alto di gestione delle crisi:
- attivare altri rilevanti moduli/processi di gestione delle crisi dell'intermediario.

f) Transactions affected - High impact (*Transazioni interessate – Alto impatto*)

Nel caso di incidente che coinvolge servizi di pagamento dell'intermediario, il numero di transazioni interessate è maggiore del 25% del livello normale delle transazioni dell'intermediario (in termini di numero di transazioni) o di 15 milioni di EUR.

L'intermediario/entità del gruppo 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, l'intermediario/entità del gruppo 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, l'intermediario/entità del gruppo 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. Se l'intermediario non ritiene che tale dato sia rappresentativo (ad esempio, a causa della stagionalità), può utilizzare un'altra metrica, più

rappresentativa, e comunicare la motivazione alla base di tale approccio compilando il campo corrispondente dei commenti del modulo.

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

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

L'intermediario/entità del gruppo 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.

L'intermediario/entità del gruppo considera come «utenti del servizio» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con l'intermediario interessato che garantisce loro l'accesso al servizio interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. L'intermediario 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 di un intermediario che offre servizi operativi a terzi, tale intermediario 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, gli intermediari considerano 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) **Concomitanza di impatti "minori": l'intermediario altresì segnala allorquando almeno tre delle seguenti quattro condizioni, valutate singolarmente come impatti "minori", si rilevino nell'ambito dei servizi di pagamento contemporaneamente:**

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

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

      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.

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

      Il numero di utenti del servizio offerto dall'intermediario 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.

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

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

   L'intermediario 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. L'intermediario 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.

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

   L'intermediario 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 la 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.

Inoltre, gli intermediari valutano 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).

Se sulla base dei precedenti criteri l'intermediario stabilisce che l'incidente non è grave, ha tuttavia la possibilità di considerarlo tale secondo criteri definiti internamente. Più precisamente, l'intermediario può comunque segnalare l'incidente alla Banca d'Italia 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, l'intermediario deve avvalersi delle valutazioni dei propri esperti per decidere se tali eventi determinino un unico incidente o corrispondano a più incidenti.

Nel caso di segnalazione di un incidente che interessi più di una entità del gruppo (e non il gruppo nel suo insieme) la capogruppo evidenzia nel modulo eventuali impatti specifici sulle singole entità del gruppo e compila i campi (i) indicando le informazioni rilevanti per ciascuna entità interessata; oppure (ii) utilizzare intervalli di valori, nei campi dove ciò è consentito, indicando il valore più basso e quello più alto osservati o stimati per le diverse entità.

4. Il modello per la segnalazione degli incidenti operativi o di sicurezza

Gli istituti devono utilizzare il modello standardizzato (cfr. documento "comunicazione_incidenti_SI_2021.pdf") per segnalare gli incidenti operativi o di sicurezza gravi.

Il modello presenta campi standard contenenti le informazioni essenziali relative all'incidente grave.

Il modello deve essere utilizzato ad ogni aggiornamento delle informazioni, in modo che sia compilato gradualmente e completato al momento dell'invio del report finale. Qualora l'intermediario lo desideri, assieme al modello è possibile fornire documentazione aggiuntiva, come le prove relative all'attacco o la documentazione dell'infrastruttura per la sicurezza oltre che la copia delle eventuali comunicazioni che sono state effettuate (o saranno effettuate) ai propri clienti, come previsto dall'articolo 96, paragrafo 1, comma 2, della PSD2.

Il modello per la segnalazione dell'incidente prevede tre categorie di campi:

- campi obbligatori per il primo report (campi rossi);
- campi obbligatori per il report ad interim (campi blu);
- campi obbligatori per il report finale (campi verdi).

Tutti i campi all'interno del modello sono obbligatori, sebbene alcuni prevedano opzioni quali *other* (altro) o *unknown* (sconosciuto). È sempre possibile anticipare la compilazione di campi relativi ad un report successivo se si possiede l'informazione e modificare campi già compilati in un report precedente se necessario.

Nell'ultima pagina del modello ("Affected Entities") vanno indicate la (le) entità del gruppo interessate dall'incidente, indicando, la denominazione, il codice ABI (o altro codice identificativo univoco nazionale, se applicabile), la nazione e la tipologia dell'entità colpita dall'incidente. Nel caso in cui l'incidente interessi la sola entità riportante non è necessario compilare la suddetta pagina.

Si forniscono di seguito una rassegna dei campi e ulteriori indicazioni per la compilazione.

Intestazione

First report: il primo report relativo all'incidente, atteso entro due ore dal momento in cui esso è stato classificato come "grave".

Interim report: il report ad interim da inviare dopo che l'attività è tornata alla normalità ma in ogni caso non oltre tre giorni lavorativi dopo il primo report (*first report*).

Final report: report finale relativo all'incidente, atteso entro 20 giorni lavorativi dalla chiusura dell'incidente (utilizzare questa opzione anche in caso di relazione di chiusura).

Report date and time: data e ora di compilazione del report

Incident ID (for interim or final report): identificativo dell'incidente, fornito da Banca d'Italia dopo l'invio del primo report, da inserire nei corrispondenti report successivi (ad interim e finale).

Changes made to previous reports (Modifiche apportate ai rapporti precedenti): indicare le modifiche apportate alle informazioni già fornite con i rapporti precedenti (es. il rapporto iniziale o, ove applicabile, il rapporto ad interim).

Incident reclassified as non-significant (incidente riclassificato come “non grave”): selezionare nei report successivi al primo, se ad un’analisi più approfondita degli impatti, la classificazione dell’incidente è stata ridotta a “non grave”, indicando eventualmente una motivazione nel campo “*Reclassification - Please explain*”.

First report - Campi rossi

General details (Informazioni generali)

- *Reporting entity - ABI code of the reporting entity* (codice ABI dell’istituto segnalante)
- *Reporting entity - Joint Supervisory Team (JST) code* (codice del *Joint Supervistory Team*, JST): il codice del JST dell’intermediario.
- *Reporting entity - Name* (Nome dell’istituto segnalante)
- Country/countries affected by the incident: paese o paesi in cui si è verificato l’incidente.
- *First and second contact person within the institution* (primo e secondo referente all’interno dell’intermediario): inserire i riferimenti di due soggetti che è possibile contattare per ricevere maggiori informazioni sull’incidente grave (a livello di gruppo e/o entità, le persone più informate sull’incidente grave segnalato). È possibile modificare i nominativi all’invio dei report ad interim e finale. Non esiste alcun requisito che imponga la compilazione del modello da parte di un soggetto specifico e non è obbligatoria la firma autorizzativa di un alto dirigente.

Incident Detection And Classification (Rilevamento e classificazione incidente)

- *Date and time of detection of the incident* (data e ora di rilevazione dell’incidente): la data e ora in cui l’incidente è stato rilevato per la prima volta. La data non deve necessariamente coincidere con la data del primo report. L’importanza di un incidente rilevato, ad esempio, può aumentare nel tempo o l’entità del problema può manifestarsi soltanto in un secondo momento.
- *Date and time of classification of the incident* (data e ora di classificazione dell’incidente): la data e ora in cui l'incidente è stato classificato come grave. Nel caso in cui il primo report venga trasmesso in ritardo (oltre le 2 ore dalla classificazione come incidente grave) i motivi di tale ritardo devono essere riportati nel campo “*Reasons for late submission first report”.*
- *Incident discovered by* (incidente rilevato da): si deve indicare chi per primo ha rilevato l’incidente.
- *Type of incident* (Tipo di incidente): selezionare l’opzione *Cyber* o *operational* (incidente operativo) una volta accertata la natura dell’incidente. Se al momento della compilazione del report non è ancora chiara la natura dell’incidente (es. se l’incidente sia dovuto ad un attacco o meno), selezionare *unknown* (sconosciuto).

- *Does the incident affect entity's payment services?* (L'incidente interessa servizi di pagamento offerti dall'intermediario?): indicare se sono stati interessati servizi di pagamento dei clienti dell'intermediario.
- *Reason for reporting the incident (motivo della segnalazione):* Scegliere uno o più criteri che hanno innescato la segnalazione dell'incidente grave. È possibile trovare maggiori informazioni sui criteri di segnalazione nella sezione 3 ("Criteri e soglie per la segnalazione") del presente documento.
- *Impact in other EU Member States, if applicable* (Impatti in altri Stati membri UE, se applicabile): indicare gli eventuali impatti che l'incidente ha avuto in un altro/i Stato/i membro/i dell'UE (ad esempio su utenti, altri intermediari e/o infrastrutture di pagamento).
- *Reporting to other authorities* (Segnalazione ad altre autorità): indicare se l'incidente è stato/sarà segnalato ad altre autorità, se noti al momento della segnalazione. In caso affermativo, specificare le predette autorità.
- *A short and general description of the incident* (Una breve e generale descrizione dell'incidente): è il campo in cui inserire le informazioni relative all'incidente grave note al momento dell'invio del primo report. È possibile rivedere e/o migliorare la descrizione sintetica all'invio dei report ad interim e finale (negli appositi campi testuali).

Interim Report - Campi blu

General details (Informazioni generali)

- *What is the specific issue?* (Qual è il problema specifico?): inserire una descrizione più dettagliata dell'incidente avendo cura di indicare almeno le sue caratteristiche principali e le informazioni sul problema specifico.
- *How did the incident start?* (Come è iniziato l'incidente?): inserire una descrizione su come l'incidente è iniziato includendo anche il background sulla rilevazione (come e chi si è accorto dell'incidente, chi ha coinvolto, ecc.).
- *How did it evolve?* (Come si è evoluto?): Indicare come l'incidente si è evoluto dopo la rilevazione.
- *What are the consequences?* (Quali sono le conseguenze?): inserire una descrizione dettagliata delle conseguenze dell'incidente, con particolare riferimento alle conseguenze per gli utenti dei servizi.
- *Was the incident communicated to payment service users?* (L'incidente è stato comunicato agli utenti del servizio di pagamento?): indicare se l'incidente è stato comunicato agli utenti del servizio di pagamento ed eventualmente fornire dei dettagli di tale comunicazione. Utilizzare il valore N.A. per gli incidenti che non hanno impatti sui servizi di pagamento.

- *Was it related to a previous incident/s?* (L'incidente è correlato a precedenti incidenti?): Indicare se l'incidente è correlato a precedenti incidenti e in caso affermativo fornire gli identificativi di quest'ultimi.
- *Date and time of beginning of the incident - if known* (data/ora a partire dalla quale l'entità è stata colpita dall'incidente - se conosciuta): data e ora in cui l'incidente è iniziato, se noto.
- *Is the incident closed?* (L'incidente è stato chiuso?): Indicare se l'incidente è stato chiuso e la data/ora di chiusura. Se l'incidente non è ancora chiuso, indicare la data/ora attesa di chiusura. Aggiornare tale campo, ove necessario, ad ogni report successivo.

Classification of the incident / Information on the incident (Classificazione e informazioni sull'incidente)

- *Cause of incident* (causa dell'incidente):
    - *Malicious actions (*Azioni malevoli): incidenti causati da azioni mirate intenzionalmente verso l'intermediario. Essi comprendono ad esempio gli attacchi *cyber*, azioni deliberate compite da personale interno, danneggiamenti causati da personale esterno, ecc.
    - *Process failure* (malfunzionamento del processo): la causa dell'incidente è stata l'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).
    - *System failure* (Malfunzionamento del sistema): la causa dell'incidente è associata con una progettazione, esecuzione, componenti, specifiche, integrazione o complessità non adeguata dei sistemi, reti, infrastrutture e banche dati che supportano le attività dell'intermediario.
    - *Human errors* (Errori umani): incidenti causati o in qualche modo correlati principalmente ad errori umani non intenzionali.
    - *External events* (Eventi esterni): la causa è associata a eventi generalmente al di fuori del controllo diretto dell'intermediario (es. calamità naturali, guasto del fornitore di servizi tecnici).
    - *Under investigation* (in fase di analisi): la causa non è ancora nota al momento dell'invio del report.
    - *Other (*Altro): la causa è diversa da quelle indicate, specificare dettagli nell'apposito campo testuale.
- *Incident category – only cyber incident* (categoria dell'incidente, nel caso di incidente cyber):
    - Un malware è un software utilizzato per ostacolare le operazioni svolte da un PC o da un dispositivo mobile, sottrarre informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata. Malware è un termine generico utilizzato per indicare varie tipologie di software ostili o intrusivi come virus, worm, Trojan horse,

ransomware, spyware, adware, scareware e altri programmi dannosi. Può assumere la forma di codici e script eseguibili, contenuti attivi e altri software.

- Social engineering (ingegneria sociale), nel contesto della sicurezza informatica, fa riferimento alla manipolazione psicologica degli individui volta ad indurre determinate azioni o a divulgare informazioni riservate. Pretexting (creazione di un pretesto) è l'atto di creare e utilizzare 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 è 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 diretti a individui o aziende specifiche sono denominati spear phishing e 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.
- Un'incidente operativo o di sicurezza può derivare da una minaccia posta dal personale interno o da un fornitore terzo (insider/third party provider threat) dal momento che dipendenti o ex dipendenti, nonché i fornitori terzi, possono danneggiare l'intermediario trascurando in qualche circostanza di attenersi alle policy di sicurezza e di diritto di accesso. Una violazione accidentale delle informazioni istituzionali da parte di un dipendente o un'infrazione intenzionale delle policy adottate possono avere un impatto grave sull'intermediario.
- Per accesso non autorizzato (unauthorised access) si intende un'ampia gamma di incidenti attraverso i quali un hacker accede intenzionalmente a reti, dati o sistemi in maniera illecita (incluso il brute-force attack, attacco a forza bruta), usa e/o modifica in modo non autorizzato tali risorse e/o compromette account e/o applicazioni. In alternativa, l'aggressore può tentare di indovinare la chiave, che solitamente è creata dalla password attraverso una funzione di derivazione.
- Un brute-force attack si verifica quando un aggressore tenta sistematicamente tutte le possibili password fino a trovare quella corretta. In alternativa, può cercare di indovinare la chiave, che solitamente è creata dalla password attraverso una funzione di derivazione. È possibile ottenere l'accesso non autorizzato attraverso l'immissione di uno script malevolo che forza un'applicazione ad aggirare i controlli fornendo così accesso a un database o apportando modifiche ai dati. Anche le vulnerabilità dei software rientrano in questa categoria come una delle modalità utili a conseguire l'accesso illecito.

- La negazione di servizi (denial of service) è un attacco che rende il servizio indisponibile agli utenti. Si verifica spesso nella veste di attacco distribuito di negazioni di servizio (distributed denial of service, DDoS), in cui la fonte dell'attacco è costituita da più indirizzi IP.
- Scanning or sniffing sono delle tecniche utilizzate dagli attaccanti per carpire informazioni e vulnerabilità dei sistemi da colpire.
- Una minaccia persistente avanzata (advanced persistent threat) è 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 (ad esempio phishing, malware) attuate per un lungo periodo di tempo.

- *Information regarding the attacker – ONLY cyber* (informazioni sull'aggressore, solo nel caso di attacco cyber): si deve segnalare ogni informazione disponibile sull'aggressore o sugli aggressori. Spuntare la casella *unknown* (sconosciuto) se non si possiede alcuna informazione.
- *Transactions affected* (transazioni interessate): nel caso di servizi di pagamento, indicare il livello di impatto sulla base dei criteri e soglie per la segnalazione, il numero di transazioni interessate, la percentuale di tali transazioni in relazione al numero di transazioni di pagamento effettuate con i servizi di pagamento interessati dall'incidente e il valore totale delle transazioni. Nel caso di incidenti operativi indicare se l'incidente ha avuto una durata maggiore, minore od uguale ad un'ora. Per queste variabili, si devono fornire valori significativi, che possono essere dati effettivi o stime (si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" per maggiori dettagli).
- *Users affected* (utenti interessati): indicare il livello di impatto sulla base dei criteri e soglie per la segnalazione, il numero totale di utenti che sono stati interessati e la percentuale di utenti del/dei servizio/i interessato/i dall'incidente rispetto al numero totale di utenti del/dei servizio/i interessato/i. Per queste variabili, fornire valori che possono essere dati effettivi o stime (si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" per maggiori dettagli).
- *Breach of security of network or information systems* (Violazione della sicurezza della rete o dei sistemi informativi): indicare se eventuali azioni dannose hanno compromesso la disponibilità, l'autenticità, l'integrità o la riservatezza della rete o dei sistemi informativi (inclusi i dati) dell'intermediario.
- *Service Downtime* (indisponibilità del servizio): indicare se un incidente comporta l'interruzione di servizi critici ovvero la cui interruzione riguarda processi aziendali critici o di rilevanza sistemica; in essi vanno sempre inclusi i servizi di pagamento.

Se l'incidente comporta l'interruzione di altri servizi essenziali, è importante considerare se l'impatto di questa interruzione è grave, consultando il seguente elenco (parziale):

- è stata colpita una parte considerevole del portafoglio clienti. Ciò accade se l'incidente riguarda un'alta percentuale di clienti oppure pochi clienti che tuttavia possiedono grande importanza per l'intermediario;
- è stata colpita una quota significativa di centri (ad esempio agenzie, sportelli, punti vendita);
- è stata colpita una quota significativa di dipendenti e impedita o almeno ostacolata la loro attività quotidiana;
- i processi aziendali si sono interrotti per un periodo di tempo considerevole in rapporto alla loro criticità (ad es. da due ore per un processo sistemico a più di un giorno per quelli meno critici).

Nel caso di impatto sui servizi di pagamento dovrà essere considerato il periodo di tempo durante il quale qualsiasi attività, processo o canale relativo alla fornitura di servizi di pagamento è o sarà probabilmente inattivo e, quindi, impedisce i) l'avvio e/o l'esecuzione di un servizio di pagamento e/o, ii) accesso a un conto pagamenti.

- *Total service downtime* (interruzione del servizio): indicare i giorni/ore/minuti di inattività del/dei servizio/i specificando se si tratta di valori stimati o reali. Nel caso di interruzione di un servizio di pagamento, l'intermediario dovrà considerare sia gli intervalli di tempo in cui è aperto per l'attività, come richiesto per l'esecuzione dei servizi di pagamento, sia gli orari di chiusura e i periodi di manutenzione, se pertinenti e applicabili. Se la data di inizio di interruzione del servizio non è conosciuta, si potrà utilizzare in via eccezionale la data in cui viene rilevata l'interruzione del servizio.
- *Economic impact* (impatto economico): l'importo deve essere espresso in euro. Si deve inserire l'ammontare delle perdite sia dirette che indirette, come fondi o beni sottratti, costi di sostituzione di hardware e software, altri costi giudiziari e di ripristino dei danni (per es. revisori esterni, negoziazione di nuovi contratti, ricerca di nuovi fornitori), sanzioni per il mancato rispetto di obblighi contrattuali, mancati ricavi dovuti alla perdita di opportunità commerciali, potenziali spese legali. I valori inseriti possono essere stimati o reali. Si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" punto b) per maggiori dettagli.
- *Was the significant cyber incident escalated internally to senior (top) management for action outside of day-to-day procedures* (l'incidente grave è stato portato, a livello interno, all'attenzione dell'alta dirigenza per un intervento al di fuori delle procedure quotidiane): si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" punto c) per maggiori dettagli.

- *Were crisis management (or equivalent) procedures activated or is it likely activated?* (Sono state attivate o è probabile che si attivino procedure di gestione della crisi?): si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" punto e) per ulteriori dettagli.
- *Were any legal or regulatory requirements breached?* (si è verificata la violazione di norme legali o regolamentari?): si veda la sezione "Criteri e soglie per la segnalazione" punto i) per ulteriori dettagli.
- *Was there any media coverage?* (l'incidente ha ricevuto attenzione mediatica?): si veda la sezione "Criteri e soglie per la segnalazione" punto a) per ulteriori dettagli.
- *Other entities (e.g., intermediaries, infrastructures) involved or potentially interested? (altri enti coinvolti nell'incidente, o potenzialmente interessati?):* selezionare se l'incidente ha avuto impatti su enti esterni e/o se altri enti potrebbero potenzialmente essere interessati dall'incidente.

Incident impact and incident mitigation (Impatto e mitigazione dell'incidente)

- *Overall impact (*impatto generale*):* indicare quali dimensioni sono state interessate dall'incidente. È possibile contrassegnare più caselle.
    - *Integrity (*Integrità): proprietà di salvaguardia dell'esattezza e della completezza delle risorse (inclusi i dati).
    - *Availability (*Disponibilità): proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento.
    - Confidentiality (Riservatezza): proprietà per cui l'informazione non è resa disponibile o divulgata a persone, entità o procedure non autorizzate.
    - Authenticity (Autenticità): proprietà di una fonte di essere quella che dichiara di essere.
- *Was the incident affecting you directly, or indirectly through a service provider? (fornitore terzo coinvolto):* indicare se l'intermediario è stato direttamente colpito dall'incidente oppure l'incidente ha colpito un fornitore terzo o un servizio esternalizzato, provocando il coinvolgimento dell'intermediario in maniera indiretta. Fornire, in quest'ultimo caso, il nome del/dei fornitori.
- *Were other service providers/third parties affected or involved? (*Altri service provider/terze parti affette o coinvolte?*):* indicare se l'incidente ha interessato o coinvolto altri fornitori di servizi/terze parti, nel caso in cui queste informazioni siano disponibili. In caso affermativo, indicarne il nome e fornire ulteriori informazioni.
- *Other impacts:*
    - *Unauthorised release of information?* (diffusione non autorizzata di informazioni?). Specificare se:

        - *Information related to the institution leaked* (sono state sottratte informazioni relative all'intermediario): informazioni strettamente riservate proprie dell'intermediario.
        - *Sensitive client information leaked* (sono state sottratte informazioni sensibili sui clienti): dati personali dei clienti quali nome, indirizzo, numeri di telefono, dati delle carte di credito e di debito.
    - *Online banking fraud (frodi relative all'internet banking):* frodi monetarie, compromissione delle credenziali dei clienti.
    - *Other impact (altro impatto):* indicare, se necessario, altri impatti dell'incidente.
- *Services and components affected* (servizi e componenti colpiti): selezionare uno o più degli elementi forniti nel modello.
- *Business lines affected (linee di business colpite):* selezionare uno o più degli elementi forniti *nel* modello. Si è seguita l'articolazione fornita in "Basilea 3: Schema di regolamentazione internazionale delle banche"[9].
- *Commercial channels affected (canali commerciali interessati):* selezionare uno o più degli elementi forniti nel modello.
- *Payment services affected (if any) (servizi di pagamento interessati):* selezionare uno o più degli elementi forniti nel modello.
- *Payment services functional areas affected (if any) (aree funzionali dei servizi di pagamento interessati):* selezionare uno o più degli elementi forniti nel modello.
- *Which actions/measures have been taken so far or are planned to recover from the incident?* (Quali azioni/misure sono state adottate finora o sono previste per il ripristino a seguito dell'incidente?): fornire informazioni dettagliate sulle azioni intraprese o pianificate per affrontare temporaneamente l'incidente.
- *Was a business continuity plan activated* (è stato attivato un piano di continuità operativa): indicare se, a seguito dell'incidente, è stato attivato il piano di continuità operativa ed eventualmente specificare i dettagli più rilevanti e la data di attivazione. Per maggiori dettagli si veda la sezione "Criteri e soglie per la segnalazione" punto e).
- *Was a disaster recovery plan activated* (è stato attivato un piano di disaster recovery): indicare se, a seguito dell'incidente, è stato attivato il piano di *disaster recovery* ed eventualmente specificare i dettagli più rilevanti e la data di attivazione.

Investigation, mitigation and resolution of the incident (analisi, misure di mitigazione e soluzione dell'incidente)

[9] "Basilea 3: Schema di regolamentazione internazionale per il rafforzamento delle banche e dei sistemi bancari", Banca dei Regolamenti Internazionali (BRI), dicembre 2010.

- *Has the intermediary cancelled or weakened some controls because of the incident?* (è stata annullata o attenuata l'intensità di alcune misure di controllo a causa dell'incidente?): indicare se sono state rimosse alcune misure di controllo (ad esempio, interrompendo l'applicazione del principio del doppio controllo) per affrontare l'incidente e, in caso affermativo, fornire dettagli relativi alle motivazioni alla base dell'attenuazione o dell'annullamento delle misure di controllo.

Final Report - Campi verdi

General details (Informazioni generali)

- *Additional information* (informazioni aggiuntive): fornire informazioni dettagliate relative all'incidente grave e note al momento dell'invio del report finale. Si devono aggiungere informazioni più approfondite sull'incidente, aggiornando, eventualmente, quelle fornite nel report ad interim, nonché un'accurata analisi delle cause.
- *Are all original controls in place?* (Tutti i controlli originali sono ripristinati?): Indicare se le misure di controllo eventualmente rimosse o attenuate per far fronte all'incidente sono state tutte ripristinate, in caso negativo indicare le misure ancora non ripristinate e la data in cui si prevede il loro ripristino. Se nessuna misura di controllo è stata rimossa/attenuata durante l'incidente selezionare la voce "*Original controls were never cancelled or weakened*" (I controlli originali non sono stati mai cancellati o attenuati).

Root cause - follow up and additional information (Causa principale – follow-up e informazioni aggiuntive)

- *Root cause and/or Vulnerabilities/weaknesses identified – only for operational incidents* (Causa all'origine dell'incidente e/o vulnerabilità/debolezze identificate – solo per incidenti operativi): nel caso di incidenti operativi, indicare qual è la causa principale dell'incidente e/o le eventuali vulnerabilità/debolezze identificate e qui di seguito descritte. Se ancora non note, indicare la/le più probabile/i. È possibile selezionare più scelte. L'elenco non è inteso essere esaustivo e non preclude la possibilità per gli istituti di considerare altri punti di debolezza e intraprendere le azioni ritenute più appropriate a seconda delle specifiche circostanze dell'incidente.
    - *Deficient monitoring and control* (Monitoraggio e controllo carenti): carenze nei processi di monitoraggio e controllo ad esempio in relazione alle operazioni in esecuzione, alla scadenza di certificati, alla scadenza di licenze, alle scadenze delle patch, alla definizione dei valori massimi di contatori, ai livelli di riempimento del database, alla gestione dei diritti utente, al principio del doppio controllo.

- *Communication issues* (Problemi di comunicazione): problemi di comunicazione ad es. tra operatori di mercato o all'interno dell'organizzazione;
- *Improper Operations* (Operazioni improprie): riscontrate operazioni non valide come ad es. mancato scambio di certificati, cache piena, ecc.
- *Inadequate Change management* (Gestione del cambiamento inadeguata): Inadeguatezza del processo di *change management* (gestione del cambiamento) evidenziata ad es. da errori di configurazione non identificati, problemi con il roll-out (inclusi aggiornamenti), problemi di manutenzione, errori imprevisti.
- *Inadequacy of internal procedures and documentation* (Inadeguatezza delle procedure interne e della documentazione): procedure interne e/o documentazione non adeguate (es. mancanza di trasparenza in merito a funzionalità, processi e insorgenza di malfunzionamenti, assenza di documentazione, ecc.).
- *Recovery issues* (Problemi di ripristino): Problemi con il processo di *recovery*, quali ad es. gestione delle emergenze, ridondanza inadeguata, ecc.
- *Hardware failure* (Malfunzionamento *hardware*): guasto dell'apparecchiatura tecnologica fisica che esegue i processi e/o archivia i dati necessari all'intermediario per svolgere la propria attività.
- *Network failure* (Malfunzionamento rete): guasto delle reti di telecomunicazione, pubbliche o private, che consentono lo scambio di dati e informazioni (ad es. tramite Internet).
- *Database issues* (Malfunzionamenti database): problemi con la struttura dei dati che memorizza le informazioni/i dati necessari all'intermediario per svolgere la propria attività.
- *Software/application failure* (Malfunzionamenti *software*/applicativi): guasti di programmi, sistemi operativi, ecc. che supportano l'erogazione dei servizi da parte dell'intermediario (es. malfunzionamenti, funzioni sconosciute).
- *Physical damage* (Danno fisici): ad es. danni involontari causati da condizioni inadeguate, lavori di costruzione.
- *Unintentional human activity* (Atto umano non intenzionale): ad es. disattenzioni, errori, omissioni, mancanza di esperienza e conoscenza.
- *Human inaction* (Mancata azione umana): ad es. per mancanza di competenze, conoscenze, esperienze, consapevolezza.
- *Insufficient human resource* (Risorse umane insufficienti): ad es. mancanza di risorse umane, disponibilità di personale.
- *Force majeure* (Causa di forza maggiore): ad es. mancanza di corrente, incendi, cause naturali come terremoti, inondazioni, forti precipitazioni, vento forte.

- *Failure of a supplier/technical service provider* (Inadempienza di un fornitore/prestatore di servizi tecnici): ad es. interruzione di corrente, interruzione di Internet, problemi legali, problemi aziendali, dipendenze dal servizio.
- *Deliberate internal actions* (Atto interno volontario): ad es. sabotaggio, furto.
- *Deliberate external physical damage* (Danno fisico volontario esterno): ad esempio sabotaggio, attacco fisico dei locali/data center.
- *Other* (Altro): Nessuna delle voci sopra elencate. Specificare meglio nell'apposito campo di testo libero.

- *Root cause and/or Vulnerabilities/weaknesses identified – only for cyber incidents* (Causa all'origine dell'incidente e/o vulnerabilità/debolezze identificate – solo per incidenti *cyber*): nel caso di incidenti *cyber*, indicare qual è la causa principale dell'incidente e/o le eventuali vulnerabilità/debolezze identificate. Se ancora non note, indicare la/le più probabile/i. È possibile selezionare più scelte. L'elenco non è inteso essere esaustivo e non preclude la possibilità per gli istituti di considerare altri punti di debolezza e intraprendere le azioni ritenute più appropriate a seconda delle specifiche circostanze dell'incidente.
  - *Inadequate patch management* (gestione inadeguata delle patch): la gestione delle patch è un settore della gestione dei sistemi che include l'acquisizione, il collaudo e l'installazione di patch multiple (cambiamenti di codice) ad un sistema informatico amministrato. Le funzioni del processo di gestione delle patch comprendono: mantenere la conoscenza attuale delle patch disponibili, decidere quali patch siano adeguate a specifici sistemi, garantire che le patch siano correttamente installate, collaudare i sistemi dopo l'installazione e documentare tutte le procedure associate, come specifiche configurazioni richieste.
  - *Unauthorised software/wrong version* (software non autorizzato/versione non corretta): carenze nella lista dei programmi e delle versioni autorizzati.
  - *Inadequate privileged account management* (gestione inadeguata degli account privilegiati): l'utilizzo improprio dei privilegi da amministratore è uno dei principali metodi usati dagli aggressori per diffondersi all'interno dell'entità prescelta.
  - *Inadequate email/web browser protection* (protezione di e-mail/browser web inadeguata): i browser web e i client di posta elettronica sono punti di ingresso e di aggressione molto comuni a causa della loro alta flessibilità e complessità tecnica e della loro interazione diretta con utenti e altri sistemi e siti web.
  - *Inadequate malware defences* (difese inadeguate dai malware): carenze nei meccanismi utilizzati per impedire l'installazione, la diffusione e l'esecuzione di codici dannosi.

- *Inadequate identity access management* (gestione inadeguata degli accessi basati sull'identità): i processi e gli strumenti per seguire/controllare/impedire/correggere l'accesso sicuro a elementi critici (ad esempio informazioni, risorse, sistemi) in linea con l'individuazione formale delle persone, dei PC e delle applicazioni che hanno necessità e diritto di accedervi sulla base di una classificazione approvata. Tutte le comunicazioni contenenti informazioni sensibili che passano attraverso reti meno affidabili dovrebbero essere crittografate.
- *Inadequate security configurations for secure hardware and software on devices, laptops, workstations and servers* (configurazioni di sicurezza inadeguate a proteggere hardware e software su dispositivi, laptop, postazioni di lavoro e server).
- *Inadequate boundary defences* (difese perimetrali inadeguate): gli aggressori si impegnano a sfruttare i sistemi raggiungibili tramite internet, non solo la rete perimetrale ma anche i PC delle postazioni di lavoro e i laptop che scaricano contenuti da internet attraversando il perimetro della rete.
- *Inadequate control of network ports, protocols and services* (controllo inadeguato di porte, protocolli e servizi di rete): può indurre l'utilizzo illecito da parte degli aggressori.
- *Inadequate resilience and/or back-up of systems or files* (inadeguata capacità di recupero resistenza e/o backup inadeguati di sistemi o file).
- *Unsecured network devices (firewalls, routers, switches)* (dispositivi di rete non sicuri (firewall, router, switch)).
- *Inadequate maintenance and monitoring of logs* (manutenzione e monitoraggio dei log inadeguati): carenze nell'analisi e nei log di sicurezza possono consentire agli aggressori di celare la loro posizione, i loro software dannosi e le loro attività sui dispositivi delle vittime.
- *Inadequate application software security controls (web-based and other applications)* (controlli di sicurezza dei software applicativi inadeguati (applicazioni basate sul web e altre)). Le vulnerabilità possono essere imputabili a varie ragioni, tra le quali errori di elaborazione del software, errori logici, requisiti incompleti e reazioni non conformi a circostanze insolite o impreviste. Esempi di errori specifici sono, tra gli altri: l'incapacità di controllare la quantità di dati inseriti dall'utente; l'impossibilità di filtrare dai flussi in ingresso le sequenze di caratteri non necessarie ma potenzialmente dannose; la mancata inizializzazione e cancellazione delle variabili; una gestione carente della memoria tale da consentire ad anomalie presenti in una parte del software di diffondersi a porzioni non correlate (e più critiche sotto il profilo della sicurezza). Gli aggressori possono immettere *exploit* specifici, tra cui *buffer overflow*, *SQL injection*,

cross-site scripting, *cross-site request forgery* e *click-jacking* per assumere il controllo di dispositivi vulnerabili.

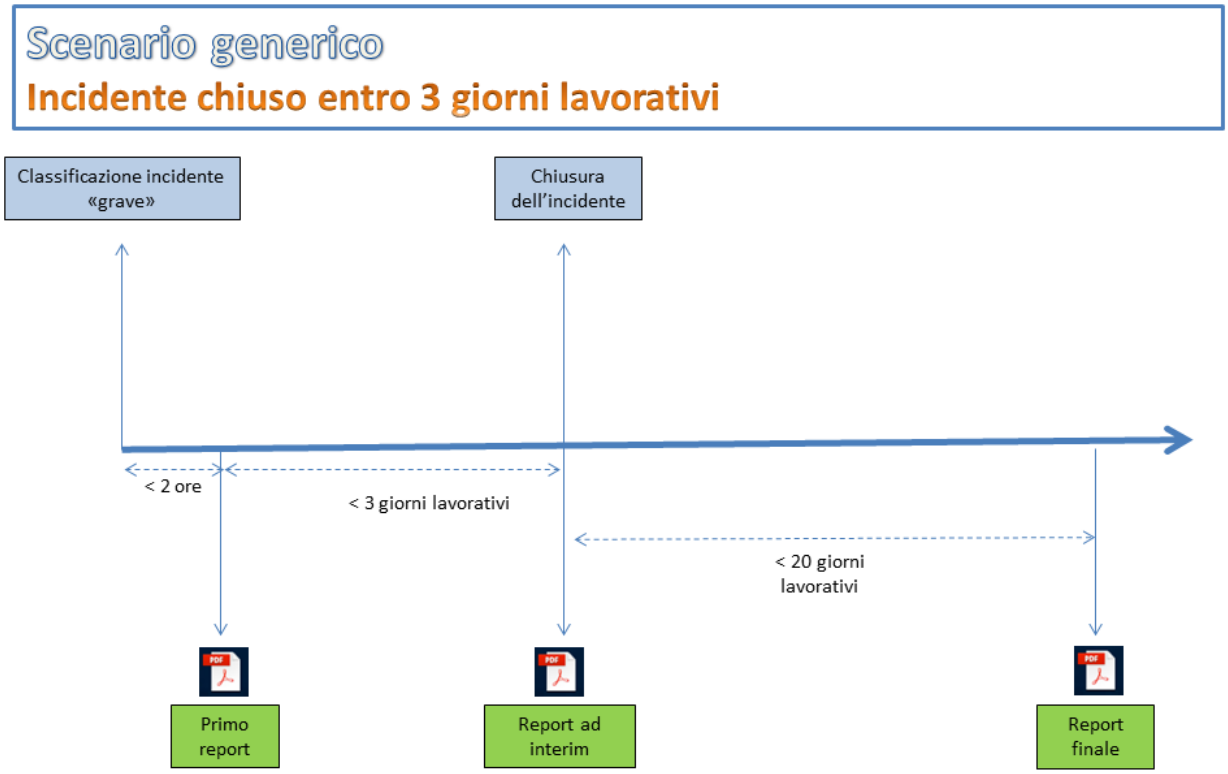
- *Inadequate DDoS defences* (difese inadeguate contro i DDoS): è possibile evitare gli attacchi DDoS bloccando in ingresso il traffico identificato come dannoso, reindirizzando il traffico attraverso server di backup e l'installazione di firewall.
- *Inadequate penetration and security testing* (test di penetrazione e sicurezza inadeguati): gli attacchi informatici hanno sfruttato vulnerabilità che sarebbe stato possibile individuare con un programma sistematico di test di penetrazione.
- *Inadequate network segmentation* (segmentazione della rete inadeguata): la segmentazione della rete è l'atto o il processo di suddivisione di una rete informatica in sottoreti, costituite ciascuna da un segmento di rete, allo scopo di migliorare la sicurezza (i broadcast saranno limitati alla rete locale e la struttura interna della rete non sarà visibile dall'esterno). Quando un criminale informatico accede illecitamente a un segmento della rete, le debolezze nella segmentazione possono consentire agli hacker di operare ulteriori movimenti all'interno della stessa.
- *Lack of staff awareness of policies* (scarsa consapevolezza delle policy da parte dei dipendenti): le azioni delle persone hanno un ruolo cruciale nella riuscita o nell'insuccesso di un'organizzazione. Le persone svolgono funzioni importanti in ogni fase relativa a progettazione, implementazione, funzionamento, utilizzo e supervisione del sistema. Tra loro, ad esempio, figurano gli sviluppatori di sistemi e i programmatori, i professionisti IT e gli utenti finali. L'errore umano può essere attribuibile anche a una mancata consapevolezza da parte dei i dipendenti/utenti delle policy dell'organizzazione. Questi errori possono portare a gravi violazioni delle informazioni o a guasti del sistema e avere ripercussioni significative sull'organizzazione.
- *Other* (Altro): Nessuna delle voci sopra elencate. Specificare meglio nell'apposito campo di testo libero.

- *Other relevant information on the root cause* (Altre informazioni rilevanti sulla causa all'origine dell'incidente): fornire eventuali ulteriori dettagli sulla causa all'origine dell'incidente, comprese le conclusioni preliminari tratte dalla relativa analisi .
- *What was the entry vector of the incident? - only for cyber incidents* (Qual è stato il vettore di ingresso dell'incidente – solo nel caso di incidenti cyber): è il percorso o il mezzo attraverso il quale un hacker si inserisce in un sistema o in una rete per accedere o estrarre dati o per attuare cambiamenti non autorizzati a un'applicazione. I vettori di attacco includono il sito web dell'intermediario, le e-mail, l'uso di dispositivi perduti o rubati, lo scambio di messaggi istantanei, le reti di terzi collegate agli istituti, le chat room e i social media eventualmente utilizzati dai dipendenti, i telefoni, i dispositivi non autorizzati. È anche possibile che per

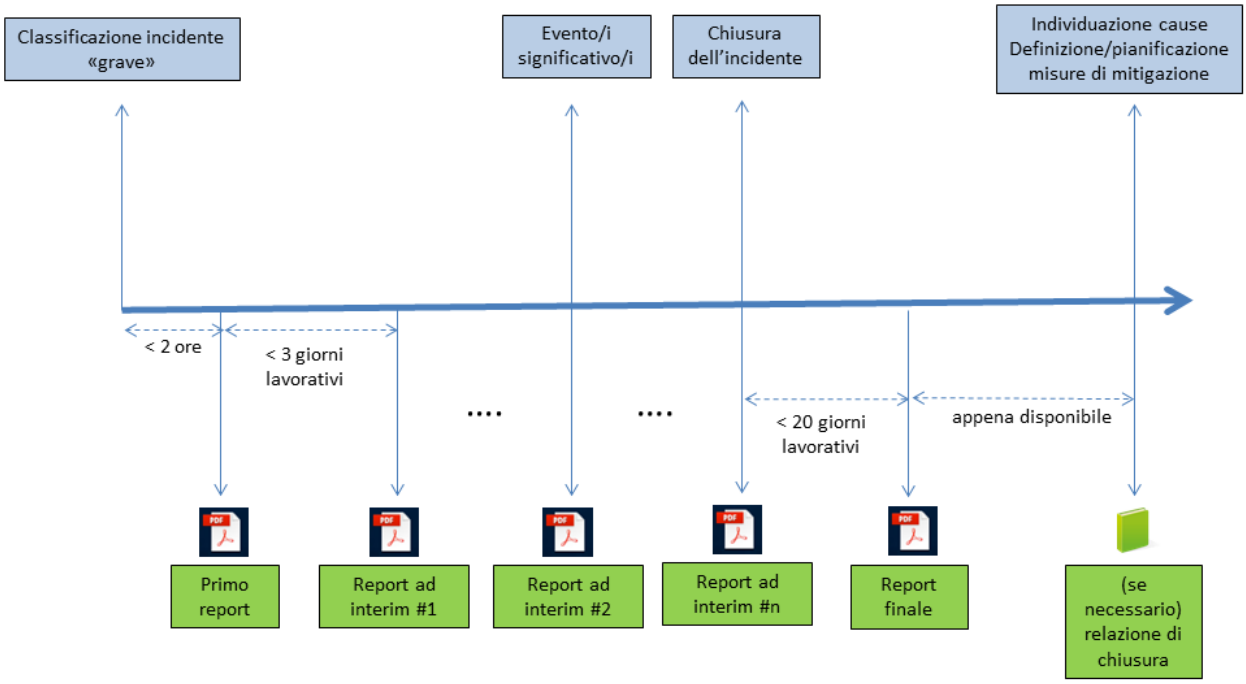
condurre l’attacco l’hacker utilizzi i regolari diritti di accesso di amministratore di un dipendente o di un fornitore dell'intermediario.

- *Main corrective actions/measures taken/planned to prevent the incident from happening again in the future, if already known* (Principali azioni correttive/misure adottate o pianificate per impedire che l’incidente si verifichi nuovamente in futuro, se già note): descrivere le principali azioni intraprese o previste per evitare il ripetersi dell’incidente in futuro.
- *Who is leading the investigation of the incident?* (quale soggetto guida l’analisi dell’incidente?)
- *Who is leading the remediation actions?* (quale soggetto guida le azioni di rimedio?)
- *Police/other security agencies involved in the investigation?* (E’ stata coinvolta la polizia o altre istituzioni di sicurezza nell’analisi dell’incidente?)
- *Was the incident reported to the national CERT/CSIRT?* (L’incidente è stato segnalato al CERT/CSIRT nazionale?).
- *Has the incident been shared with other financial intermediaries for information purposes? And with the CertFIN? If so, please provide details* (Le informazioni sull’incidente sono state condivise con altri intermediari finanziari? E con il CERTFIN?):
- *Has any legal action been taken against the group? If so, please provide details* (Sono state intraprese azioni legali contro il gruppo o entità del gruppo?): indicare se l’intermediario è a conoscenza di azioni legale intraprese nei propri confronti a seguito dell’incidente.
- *Assessment of the effectiveness of the action taken* (Valutazione dell’efficacia delle azioni intraprese): indicare il risultato di un'autovalutazione dell'efficacia delle azioni intraprese durante la durata dell'incidente, comprese le lezioni apprese dall'incidente, motivando, se del caso, il risultato nell’apposito campo testuale.

ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione

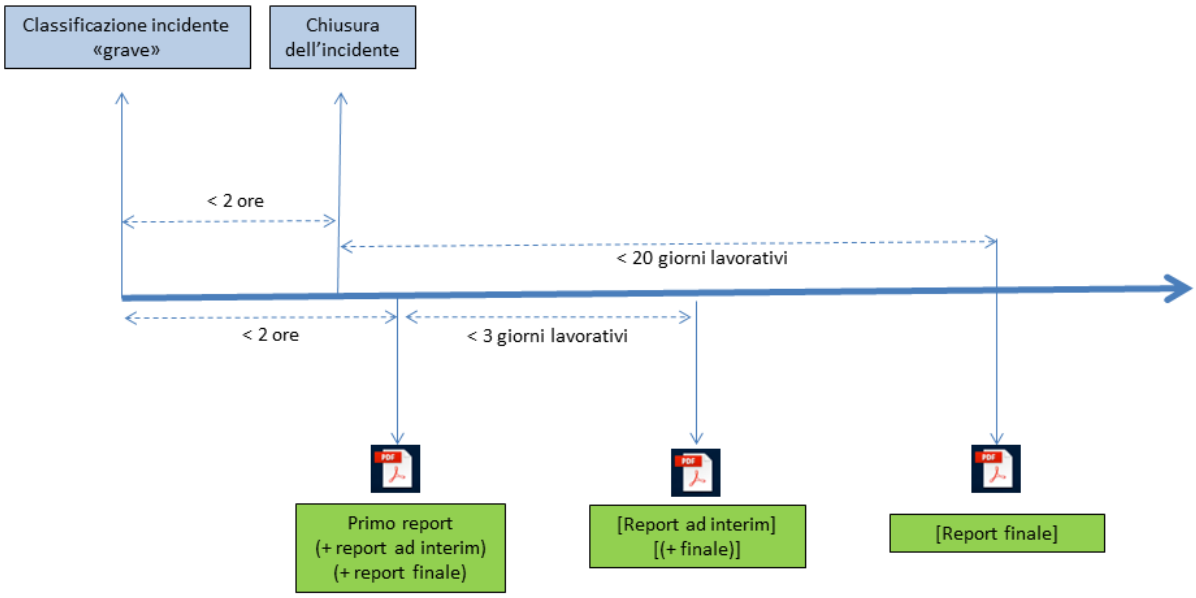


Scenario #1
Incidente chiuso dopo 3 giorni lavorativi + cause individuate dopo il report finale



- In caso di chiusura incidente dopo 3 giorni lavorativi, l'intermediario invia un report ad interim entro tre giorni lavorativi dal primo report. Invia degli aggiornamenti ogni evento significativo di cui è a conoscenza (e tra questi rientra la chiusura dell'incidente) senza vincoli temporali rispetto al precedente report

Scenario #2
Incidente chiuso entro 2 ore



- In caso di chiusura dell'incidente entro due ore l'intermediario dovrebbe adoperarsi per inviare un unico report contenente tutte le informazioni al momento in suo possesso e relative al primo report, al report ad interim ed eventualmente al report finale
- Nel caso l'intermediario non riuscisse ad inviare un unico report cumulativo, il report ad interim va trasmesso nel più breve tempo possibile ma non oltre i 3 giorni lavorativi rispetto al primo report mentre le informazioni relative al report finale (se non trasmesse congiuntamente al report ad interim) vanno trasmesse entro 20 giorni lavorativi dalla chiusura dell'incidente