BANCA D'ITALIA
EUROSISTEMA

ISTRUZIONI PER LA SEGNALAZIONE DEI GRAVI INCIDENTI DI SICUREZZA INFORMATICA – BANCHE SIGNIFICANT

Le presenti istruzioni definiscono i criteri per la valutazione di gravità di un incidente di sicurezza informatica e indicano le modalità per la segnalazione dei gravi incidenti ai sensi della Circ. n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, Tit. IV, Cap. 4). La Banca d'Italia inoltrerà alla Banca centrale europea e/o all'Autorità bancaria europea le comunicazioni ricevute, laddove previsto dalla procedura definita in ambito SSM per la segnalazione di incidenti cyber e dalla procedura definita dall'EBA per la segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2).

Gli intermediari si adeguano alla segnalazione, secondo le istruzioni qui riportate, entro la data del 1 settembre 2019.

Indice

1. Definizioni

1.1. La Circ. n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, Tit. IV, Cap. 4, Sez. 1, Par. 3), definisce **incidente di sicurezza informatica** ogni evento, o serie di eventi collegati, non pianificati dalla banca che interessa le sue risorse informatiche e che i) ha o potrebbe avere[1] un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente

[1] Tra i gravi incidenti di sicurezza informatica si escludono i c.d. *near misses,* ovvero gli eventi che grazie ai presidi di sicurezza adottati dall'intermediario non hanno causato impatti negativi sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi. Sono altresì gravi incidenti gli eventi che, sebbene al momento della rilevazione non hanno ancora prodotto impatti, potrebbero causare nell'immediato futuro un impatto negativo, in base alle previsioni dell'intermediario.

minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi)[2];

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 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.

1.4. In linea con gli Orientamenti EBA, le banche applicano le istruzioni per la segnalazione degli incidenti di sicurezza informatica anche alla segnalazione degli incidenti operativi riferiti alla prestazione dei servizi di pagamento quando non collegati al funzionamento delle risorse e dei processi ICT (cfr. Circ. n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, Tit. IV, Cap. 4, Sez. 7)).

Ai fini delle presenti istruzioni, gli eventi di sicurezza informatica sono classificati come:

- Incidenti cyber, causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzata delle risorse dell'intermediario e che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la

[2] "La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di protezione a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza)." Cfr. Circ. n. 285 - Parte Prima, Tit. IV, Cap. 4, Sez. IV, Par. 3)

continuità delle risorse e dei servizi dell'intermediario o che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario[3].

- Incidenti operativi, derivanti da processi o sistemi inadeguati o malfunzionanti, da persone o eventi di forza maggiore che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità delle risorse e dei servizi dell'intermediario. Tra tali eventi sono inclusi quelli naturali, errori software/hardware, eventi accidentali, malfunzionamenti di processo, sabotaggio (attacco fisico).

Di seguito inoltre alcune definizioni di termini adottati in questo 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.
- Continuità: Proprietà delle procedure, attività e risorse di un'organizzazione funzionali all'erogazione dei servizi finanziari e di pagamento, di essere pienamente fruibili e operativi a livelli di servizio accettabili e predefiniti.
- 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 i gravi incidenti di sicurezza informatica avuto riguardo a tutti i servizi erogati e, per la prestazione dei servizi di pagamento, anche i gravi incidenti operativi (non collegati al funzionamento delle risorse informatiche - cfr par. 1.4), a prescindere dal fatto che si verifichino presso succursali o affiliate all'interno o al di fuori dell'area dell'euro[4]. Queste due fattispecie di incidente sono di seguito indicati come "incidente".

[3] La diffusione e/o l'alterazione involontaria, per errore umano o malfunzionamento software, di dati riservati della clientela e/o dell'intermediario ricade nella categoria degli incidenti cyber.

[4] Le istruzioni si applicano anche se il grave incidente operativo o di sicurezza informatica ha origine al di fuori dell'Italia (ad esempio, quando un incidente ha origine presso la società capogruppo o una succursale costituita al di fuori dell'Italia) e ad esempio riguarda i servizi di pagamento forniti da un prestatore 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).

Per ogni incidente la segnalazione consta di tre tipologie di rapporti[5]:

- 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 include nel primo rapporto 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'intermediario include nel rapporto iniziale anche la data del successivo aggiornamento, che deve essere fornito il prima possibile e in nessun caso oltre i tre giorni lavorativi successivi.

- i report ad interim attesi entro 3 giorni lavorativi dall'invio del precedente report (primo o precedente ad interim).

  L'intermediario invia un rapporto ad interim ogniqualvolta ritenga che vi sia un aggiornamento rilevante dello stato dell'incidente e comunque entro la data del successivo aggiornamento indicata nel rapporto precedente (primo rapporto o precedente rapporto ad interim).

  L'intermediario sottomette il primo rapporto ad interim con una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione in blu del modulo). Inoltre, l'intermediario fornisce ulteriori rapporti ad interim aggiornando le informazioni già inserite nelle sezioni rossa e blu del modulo, quando venga a conoscenza di nuove informazioni rilevanti o di cambiamenti significativi rispetto al rapporto precedente (ad esempio, se la gravità dell'incidente aumenta o diminuisce, nuove cause identificate o azioni intraprese per risolvere il problema). In ogni caso, l'intermediario presenta un rapporto ad interim quando esplicitamente richiesto dalla Banca d'Italia.

  Come nel caso dei rapporti iniziali, qualora dati effettivi non siano disponibili, l'intermediario può ricorrere a stime.

  Inoltre, l'intermediario indica in ogni rapporto la data dell'aggiornamento successivo che deve avvenire il prima possibile e in nessun caso oltre i tre giorni lavorativi. Nell'impossibilità di rispettare la data prevista per il successivo aggiornamento, l'intermediario contatta la Banca d'Italia per spiegare i motivi del ritardo, proporre un nuovo termine di presentazione plausibile (non oltre i tre giorni lavorativi successivi) e inviare un nuovo rapporto ad interim, aggiornando esclusivamente le informazioni relative alla data stimata per l'aggiornamento successivo.

  L'intermediario invia l'ultimo rapporto ad interim quando le normali operazioni sono state ripristinate e l'attività è tornata alla normalità (chiusura dell'incidente), 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

[5] I rapporti dovranno essere compilati nella stessa lingua utilizzata per le comunicazioni con BCE.

(SLA), in termini di tempi di elaborazione, capacità, requisiti di sicurezza, ecc., e le misure di emergenza non sono più in vigore.

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 rapporto iniziale sia l'ultimo rapporto ad interim (ossia compilando le sezioni rossa e blu del modulo) entro le due ore previste per l'invio del primo report.

- il report finale, atteso entro 2 settimane dal momento in cui si considera che le attività siano tornate alla normalità.

  Il report 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. Nel report finale devono essere compilati i campi in verde. Laddove si necessiti di una proroga del termine di due settimane (ad esempio, se non sono ancora disponibili dati effettivi sull'impatto) si deve contattare la Banca d'Italia prima della scadenza di suddetto termine e si deve fornire una giustificazione adeguata per il ritardo e una nuova data stimata per il rapporto finale.

  Nel caso il report finale non includa tutte le informazioni necessarie perché non disponibili nei tempi richiesti (due settimane 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.

Il modulo da utilizzare per i suddetti report è annesso alle presenti istruzioni (cfr. documento "comunicazione_incidenti_SI_2019.pdf"). L'intermediario, laddove lo ritenga necessario, può integrare il modulo standardizzato con documentazione integrativa, sotto forma di uno o più allegati.

L'intermediario invia il modulo di segnalazione dell'incidente e gli eventuali documenti allegati in forma cifrata nel caso di incidente cyber laddove ritenga che la divulgazione di informazioni contenute nel modulo possa avere significativi impatti negativi sull'intermediario stesso o altri soggetti coinvolti.

Per cifrare il modulo l'intermediario deve utilizzare tutte le chiavi di crittografia annesse alle presenti istruzioni (bdi_key1.p7b, bdi_key2.p7b, bdi_key3.p7b, bdi_key4.p7b)[6].

Ogni modulo (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

[6] 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.

messaggio dovrà indicare il rapporto allegato, il tipo di incidente segnalato e l'ente segnalante, secondo il seguente schema: "Oggetto: Com_285 - WWWW ZZZZ – XXXXX YYYYY", dove WWWW va valorizzato con "PRIMO", "INTERIM", "FINALE", "RELAZIONE" con riguardo al rapporto allegato, ZZZZ con "CYBER" o "ALTRO" a seconda del tipo di 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 via PEC (ad esempio per l'impossibilità ad utilizzare la PEC a causa dello stesso incidente) l'intermediario comunica alla casella di posta elettronica non certificata SSI_incidenti@bancaditalia.it l'urgenza di ricevere un contatto telefonico per la segnalazione dell'incidente.

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 al nostro Istituto, 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.

3. Criteri e soglie per la segnalazione

Al verificarsi di un incidente, l'intermediario ne valuta la rilevanza utilizzando i criteri di seguito specificati e classificandolo 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[7].

a) Un incidente è reso pubblico e/o può comportare importanti danni reputazionali

E' 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.

[7] 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 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.

b) L'impatto finanziario stimato dell'incidente 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 su base consolidata 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 es. 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) La gestione dell'incidente è soggetta ad un'escalation[8] che lo porta, internamente, all'attenzione del responsabile aziendale per la funzione informatica (Chief Information Officer), ovvero di un livello manageriale equivalente o superiore, al di fuori del processo ordinario/periodico di relazione sugli incidenti registrati.

[8] 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).

Ad esempio, in genere il responsabile aziendale per la sicurezza informatica (*Chief Information Security Officer*, CISO) discute di solito 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, in base a quanto stabilito nelle policy e regolamenti interni .

d) L'incidente comporta verosimilmente la violazione di obblighi legali o regolamentari.

Esempi di violazione di obblighi legali o regolamentari includono, a titolo di esempio:

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

e) L'incidente innesca o potrebbe innescare procedure di gestione della continuità operativa o di gestione delle crisi.

Include i seguenti casi:

A) L'incidente provoca o potrebbe provocare l'attivazione del piano di continuità operativa (*business continuity plan*, BCP[9]) e/o l'attivazione del "CODISE (continuità di servizio)" per il coordinamento delle crisi operative della piazza finanziaria italiana.

[9] 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.

Un BCP contiene diverse procedure che possono essere innescate da un incidente, 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; 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 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, così come specificato nelle policy e nei regolamenti interni.

f) 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 5 Mln 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 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 dello schema.

g) Nel caso di incidente che coinvolge servizi di pagamento dell'intermediario, il numero di utenti del servizio interessati dall'incidente, è maggiore di 50 000 o del 25 % dei clienti dell'intermediario.

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 su dati storici per

determinare il numero di utenti del servizio interessato dall'incidente che potrebbero aver utilizzato il servizio nel corso dell'incidente.

h) **Concomitanza di impatti "minori": nel caso di incidente che coinvolge servizi di pagamento dell'intermediario, questi segnala allorquando le seguenti tre condizioni, valutate singolarmente come impatti "minori", si rilevino:**
   a. **il numero di transazioni interessate è maggiore del 10% del livello normale delle transazioni dell'intermediario (in termini di numero di transazioni) e di EUR 100.000.**
   b. **Il numero di utenti del servizio offerto dall'intermediario interessati dall'incidente è maggiore di 5.000 e del 10% dei clienti dell'intermediario.**
   c. **Il periodo di indisponibilità del servizio di pagamento è maggiore di 2 ore.**

   Quanto al punto c., 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.

i) **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 es. 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.

j) L'incidente è comunicato al CERT (Cyber Emergence Response Team) nazionale o al Cyber Security Incident Response Team (CSIRT), ad un'agenzia di sicurezza governativa o alla polizia

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 nelle policy e nei regolamenti. 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.

Il modello per la segnalazione degli incidenti contiene nell'ultima pagina una tabella ("Affected Entities") dove va indicata la lista delle singole entità del gruppo interessate dall'incidente (da compilare in ogni caso, sia che l'incidente colpisca il gruppo nel suo insieme, sia che solo una o più entità siano interessate dall'incidente).

4. Il modello per la segnalazione degli incidenti

Gli istituti devono utilizzare il modello standardizzato (cfr. documento "comunicazione_incidenti_SI_2019.pdf") per segnalare gli incidenti 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.

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

- campi obbligatori per il primo report (campi rossi);
- campi obbligatori per i report ad interim (campi azzurri);
- 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 (quando applicabile), la nazione e la tipologia dell'entità colpita dall'incidente.

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

Intestazione – tipo di report, data, identificativo dell'incidente

*First report***:** il primo report relativo all'incidente, atteso entro due ore al momento in cui esso è stato rilevato come "grave")

*Interim report***:** i successivi report relativi all'incidente (report ad interim), attesi entro 3 giorni lavorativi dall'invio del primo report o dei precedenti report ad interim)

Last interim report: ultimo report ad interim, da inviare dopo che la l'attività è tornata alla normalità

*Final report***:** report finale relativo all'incidente, atteso entro 2 settimane dalla chiusura dell'incidente. Utilizzare questa opzione anche nel caso di "Relazione" conclusiva.

*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).

Estimated time for the next update (momento stimato del prossimo aggiornamento): indicare data e ora stimate per la presentazione dell'aggiornamento successivo (rapporto ad interim, finale, relazione conclusiva)

Next update – please explain (prossimo aggiornamento - dettagli): indicare, se necessario, le ragioni della tempistica proposta per l'aggiornamento successivo

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

Campi rossi - Primo report

- *Reporting entity - Joint Supervisory Team (JST) code* (codice del *Joint Supervistory Team*, JST): il codice del JST dell’intermediario.
- *Reporting entity - ABI code of the reporting entity* (codice ABI dell’ente segnalante)
- *Reporting entity - Authorization number: indicare il numero di matricola di iscrizione all’Albo dellìentità segnalante*
- *Country/countries affected by the incident*: paese o paesi interessati dall’incidente (ad esempio, sono interessate diverse succursali del gruppo situate in vari Stati).
- *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 date/time* (data e ora di rilevazione dell’incidente): la data e ora in cui l’incidente grave 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.
- *Incident discovered by* (incidente rilevato da): si deve indicare chi per primo ha segnalato l’incidente.
- *Incident category* (categoria dell’incidente): selezionare l’opzione *Cyber* o *operational* (incidente operazionale) una volta accertata la natura dell’incidente. Se al momento della compilazione del report non è chiaro se l’incidente sia dovuto ad un attacco, 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.
- *General description of the incident* (descrizione generale 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 (sono predisposti campi distinti).

Campi azzurri – Report ad interim

- *Date/time of beginning of the incident (if known):* (la data/ora a partire dalla quale l'entità è stata colpita dall'incidente è conosciuta?): data e ora in cui l'incidente è iniziato, se noto.
- *Incident status* (status dell'incidente):
    - Diagnosi: le caratteristiche dell'incidente sono appena state identificate.
    - Riparazione: gli elementi impattati sono in riconfigurazione.
    - Recupero: gli elementi impattati vengono ripristinati all'ultimo salvataggio recuperabile.
    - Ripristino: i servizi connessi ai pagamenti sono nuovamente forniti.
- *Is the incident closed?* (L'incidente è stato chiuso?): Indicare se l'incidente è stato chiuso e data/ora di chiusura. Se l'incidente non è ancora chiuso, indicare la data/ora attesa di chiusura. Aggiornare tale campo, ove necessario, nei report ad interim e finale.
- *Detailed description of the incident* (descrizione dettagliata dell'incidente): fornire informazioni dettagliate relative all'incidente grave e note al momento dell'invio del report ad interim. È possibile rivedere e/o migliorare la descrizione all'invio del report finale.

Information on the incident (informazioni sull'incidente)

- *Was the incident affecting you directly, or indirectly through a service provider? (fornitore terzo coinvolto):* si deve spuntare questa casella se un fornitore terzo o un servizio esternalizzato è stato direttamente colpito dall'incidente, provocando il coinvolgimento dell'intermediario in maniera indiretta. Fornire, nel caso, il nome del/dei fornitori.
- *Incident type - cyber* (tipo di incidente, nel caso di attacco 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 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). 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.
- 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 es. phishing, malware) attuate per un lungo periodo di tempo.

- *Incident type – operational incidents* (tipo di incidente, nel caso incidenti di sicurezza diversi dagli attacchi cyber):
    - *Accidental* (eventi accidentali): incidenti causati da eventi accidentali, come ad esempio errori umani), ad eccezione di "data breach/corruption", classificati in questo contesto come incidenti cyber.
    - *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).
    - *SW problem* (problema software): incidenti dovuti al malfunzionamento di programmi software applicativi o di base;
    - *HW or infrastructural problem* (problema hardware o infrastrutturale): incidenti dovuti a malfunzionamenti di sistemi e componenti hardware ovvero di reti di comunicazione o piattaforme condivise.
    - *Sabotage* (sabotaggio): sabotaggio di apparati tramite accesso fisico
    - *Natural event – disaster*: incidenti causati da cause naturali o esterne, come inondazioni, incendi, terremoti.
- *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.

Impact of the incident & reason for reporting (impatto dell'incidente e motivo della segnalazione)

L'incidente grave dovrebbe manifestare il proprio impatto attraverso uno dei seguenti effetti:

- *Overall impact (impatto generale):* indicare quali dimensioni sono state interessate dall'incidente. È possibile contrassegnare più caselle.
    - Integrità: proprietà di salvaguardia dell'esattezza e della 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 l'informazione non è resa disponibile o divulgata a persone, entità o procedure non autorizzate.
    - Autenticità: proprietà di una fonte di essere quella che dichiara di essere.

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

- *Transactions affected (transazioni interessate):* nel caso di servizi di pagamento, indicare 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. 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 numero totale di utenti che sono stati interessati e la percentuale di utenti di servizi interessati rispetto al numero totale di utenti dei servizi interessati. 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).
- *Disruption of critical service* (interruzione di servizi essenziali): se un incidente comporta l'interruzione di 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 es. 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);
    - è stato colpito un servizio critico: l'interruzione ha riguardato processi aziendali critici o di rilevanza sistemica. In essi vanno sempre inclusi i servizi di pagamento.
- *Total service downtime* (interruzione del servizio): qualora si sia verificata l'interruzione di più servizi, si deve inserire la durata di quella relativa al servizio più critico.
- *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.

- *Was the significant cyber incident escalated internally to group-level 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 del gruppo per un intervento al di fuori delle procedure quotidiane): si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" 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" per maggiori 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" per ulteriori dettagli.
- *Was there any media coverage?* (l'incidente ha ricevuto attenzione mediatica?): si veda la sezione "Criteri e soglie per la segnalazione" per ulteriori dettagli.
- *Other entities (e.g., intermediaries, infrastructures) involved or potentially interested? (altri enti coinvolti nell'incidente, o potenzialmente interessati?):* selezionare se l'incidante ha avuto impatti su enti esterni e/o se altri enti potrebbero potenzialmente essere interessati dall'incidente.
- *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.
    - *Defacing / data alteration* (modifica dell'aspetto di pagine web, modifica di dati): selezionare per indicare che l'attacco era volto a danneggiare l'immagine dell'intermediario attraverso la modifica dell'aspetto della home page del sito, di altre pagine accedute da clienti, utenti interni, terze parti, ovvero di dati di rilievo.
    - *Online banking fraud (frodi relative all'internet banking):* frodi monetarie, compromissione delle credenziali dei clienti.

- *Other frauds* (altre frodi): indicare se si tratta di altre frodi perpetrate con strumenti informatici o tecniche di social engineering.
- *Other impact (altro impatto):* indicare, se necessario, altri impatti dell'incidente.

- *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.
- *Building(s) affected (Address), if applicable (Edificio/i interessato/i (indirizzo), se applicabile):* se è interessato un edificio fisico, indicarne l'indirizzo.
- *Services and components affected* (servizi e componenti colpiti): selezionare uno o più degli elementi forniti nel modello.
- *Systems affected (sistemi interessati):* 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"[10].
- *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.
- *Staff affected (personale interessato):* indicare se l'incidente ha avuto effetti sul personale e, in caso affermativo, fornire dettagli nel campo di testo libero.

Investigation, mitigation and resolution of the incident (analisi, misure di mitigazione e soluzione dell'incidente)[11]

- *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 in caso di incidente?): fornire informazioni dettagliate sulle azioni intraprese o pianificate per affrontare temporaneamente l'incidente.

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

[11]Si noti che le informazioni sulle misure di mitigazione e soluzione dell'incidente, nel precedente modulo acquisite nel report finale, sono state in parte anticipate nel report intermedio.

- *Was a business continuity plan activated* (è stato attivato un piano di continuità operativa): si veda la sezione “Criteri e soglie per la segnalazione” per maggiori dettagli.
- *Was a disaster recovery plan activated* (è stato attivato un piano di disaster recovery): si veda la sezione “Criteri e soglie per la segnalazione” per maggiori dettagli.
- *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.

Campi verdi – Report finale

Si noti che è possibile scegliere una sola opzione per ciascuno dei campi inclusi nella sezione *Investigation and resolution of the incident* (indagine e risoluzione dell’incidente*)*, con l’eccezione dei campi *What was the entry vector of the incident?* e *Vulnerabilities/weaknesses exposed* (vulnerabilità/debolezze evidenziate) nel quale sono possibili selezioni multiple.

- *Detailed description* (descrizione dettagliata): fornire informazioni dettagliate relative all’incidente grave e note al momento dell’invio del report definitivo. Si devono aggiungere informazioni più approfondite sull’incidente, aggiornando quelle fornite nel corrispondente campo del report ad interim, nonché un’accurata analisi delle cause. Il modello suggerisce una serie di dettagli da fornire. Si deve, tuttavia, riportare qualsiasi dettaglio disponibile.
- *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?)
- *If some controls had been canceled or weakened because of the incident, are the original controls back in place?* (Le misure di controllo originali sono stati ripristinate?): laddove si sia dovuto annullare o attenuare l’intensità di alcune misure di controllo a causa dell’incidente, indicare se le misure di controllo sono nuovamente attive e fornire ulteriori informazioni nel campo di testo libero.
- *What was the root cause?* (Quale è stata la causa all’origine dell’incidente, se già nota?): spiegare qual è la causa all’origine dell’incidente o, se non ancora nota, le conclusioni preliminari tratte dall’analisi delle cause all’origine dell’incidente. E’ possibile allegare un file con informazioni dettagliate se ritenuto necessario.
- *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.

- *The entry vector of the incident - ONLY CYBER* (il vettore di ingresso dell'incidente – solo nel caso di attacco 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.
- *Vulnerabilities/weaknesses identified* (vulnerabilità/debolezze identificate): si espongono di seguito alcune debolezze nei controlli interni che possono essere evidenziate dagli incidenti. Si noti che l'obiettivo è illustrare come un incidente possa rivelare meccanismi di controllo inadeguati o insufficienti nei processi interni. 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 es. 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.

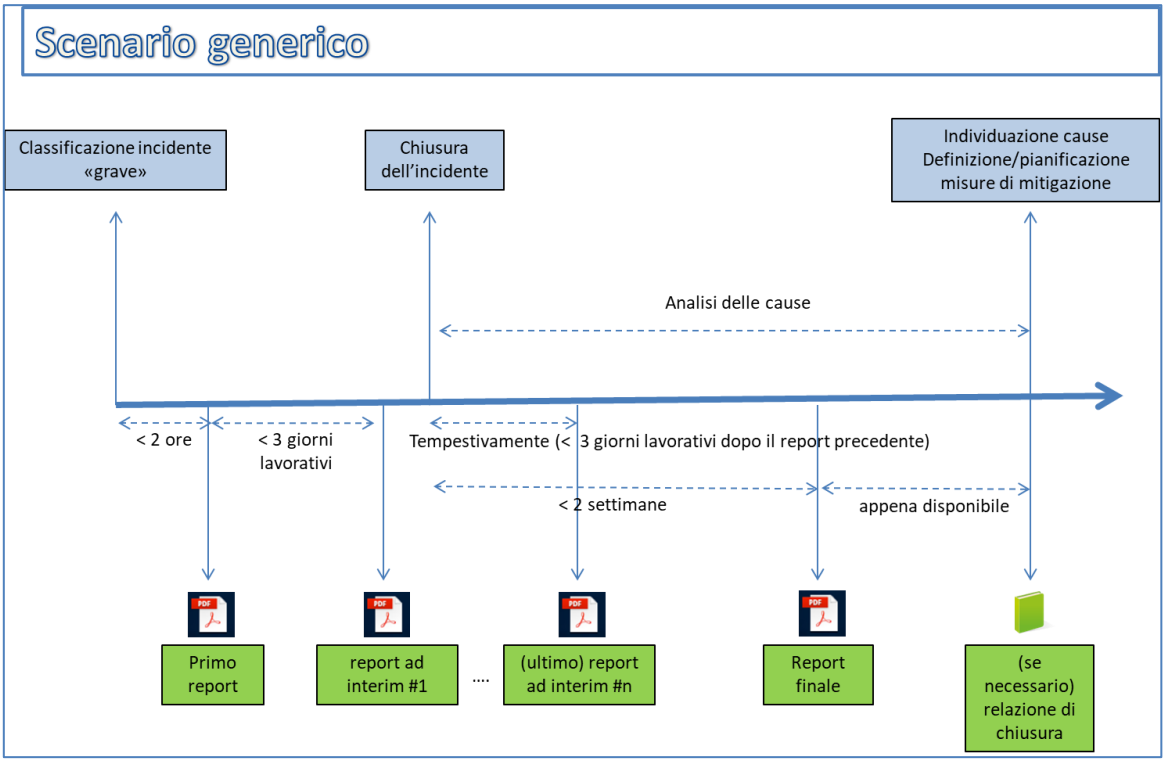
- *Inadequate penetration and security testing* (test di penetrazione e sicurezza inadeguati): gli attacchi informatici hanno sfruttato vulnerabilità che sarebbe stato possibile individuare con un programma sistematico di test di penetrazione.
- *Inadequate network segmentation* (segmentazione della 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.
- *Software bugs* (difetti del software di base o applicativo): non comprende i difetti sanati con patches rese disponibili dal produttore.
- *Hardware defects* (difetti dell'hardware di sistemi e componenti).
- *Change management issues (*problemi di gestione dei cambiamenti): problematiche riscontrate nei sistemi e nelle procedure utilizzate per il controllo delle configurazioni, dei rilasci applicativi e delle modifiche al software, inclusi i test e i collaudi prima dell'avvio in produzione.
- *Procedural issues / lack of controls* (problemi procedurali / mancanza di controlli): altri problematiche nelle procedure di gestione delle risorse IT, con particolare riguardo alla rilevazione di specifiche carenze di controlli.

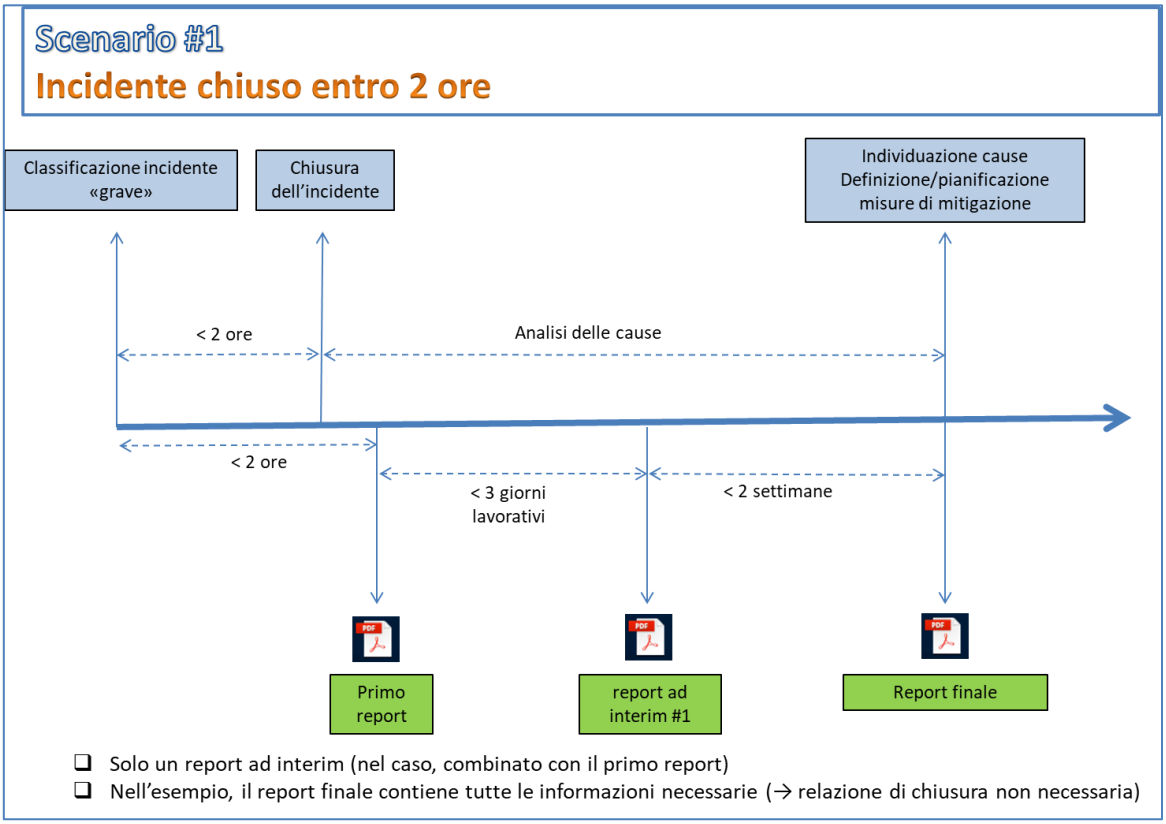
- *Are the police or other security agencies involved in the investigation?* (E' stata coinvolta la polizia o altre istituzioni di sicurezza nell'analisi dell'incidente?)
- *Was the incident reported to the national CERT/CSIRT?* (L'incidente è stato segnalato al CERT/CSIRT nazionale?).
- *Has the incident 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?)

La seconda parte del modulo ("LIST OF AFFECTED ENTITIES") va utilizzato per specificare l'elenco delle entità del gruppo direttamente interessate dall'incidente.

ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione

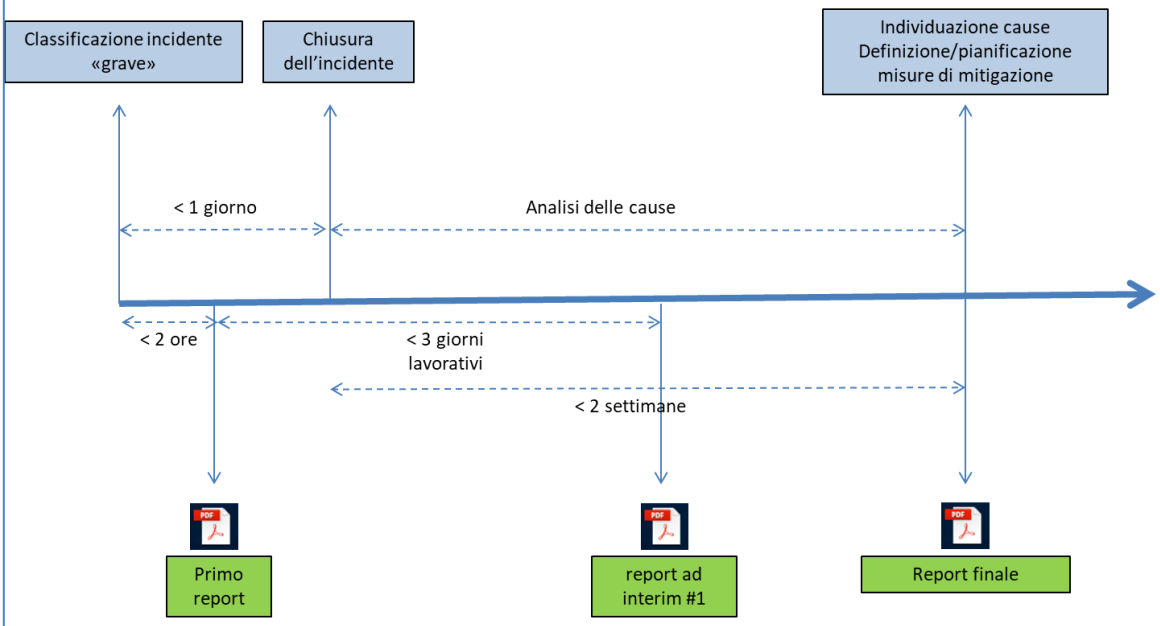




- Solo un report ad interim (nel caso, combinato con il primo report)
- Nell'esempio, il report finale contiene tutte le informazioni necessarie (→ relazione di chiusura non necessaria)

Scenario #2

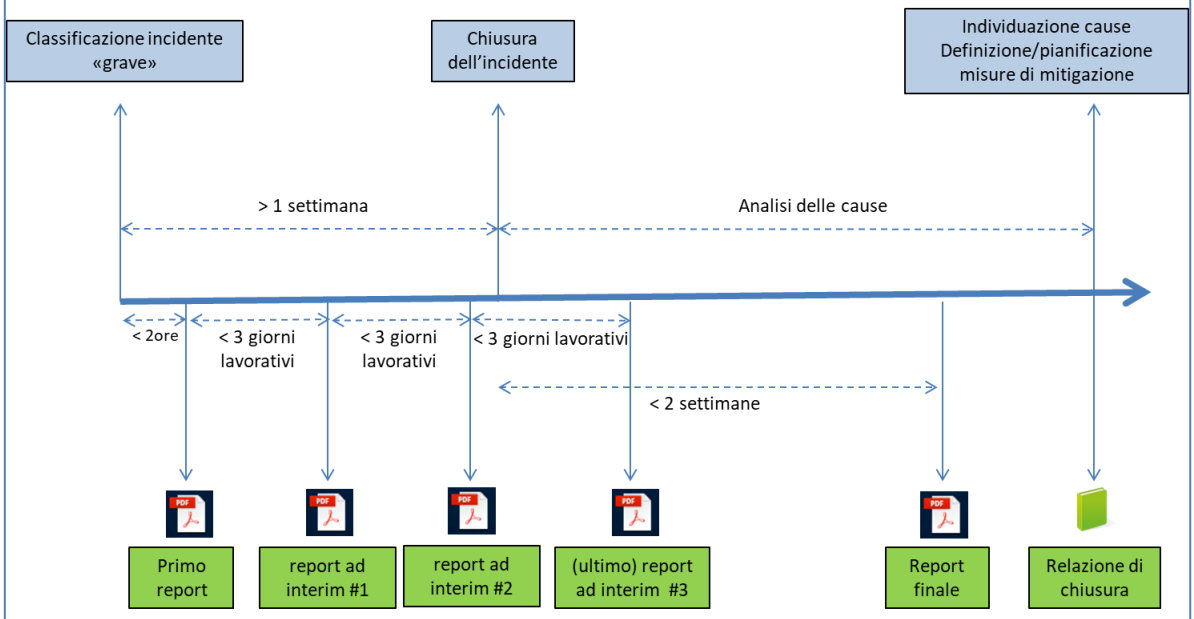
Incidente chiuso in giornata



- Solo un report ad interim necessario
- Nell'esempio, il report finale contiene tutte le informazioni necessarie (→ relazione di chiusura non necessaria)

Scenario #3

Incidente chiuso dopo oltre una settimana e fase di analisi delle cause di durata un mese



- Tre report ad interim (l'ultimo subito dopo la chiusura dell'incidente)
- Nell'esempio, il report finale non contiene tutte le informazioni necessarie (→ necessaria la relazione di chiusura)