

ISTRUZIONI PER LA SEGNALAZIONE DEI GRAVI INCIDENTI OPERATIVI O DI SICUREZZA – IP E IMEL

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 “Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica”. La Banca d'Italia inoltrerà o all'Autorità bancaria europea le comunicazioni ricevute, laddove previsto 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.	Introduzione	1
2.	Modalità di segnalazione	3
3.	Criteri e soglie per la segnalazione	5
4.	Il modello per la segnalazione degli incidenti di sicurezza informatica	9
ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione		17

1. Introduzione

Ai sensi del provvedimento della Banca d'Italia del 23 luglio 2019 “Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica” e degli “Orientamenti finali in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2)” emanati dall'ABE ivi recepiti, con “Incidente operativo o di sicurezza” si intende “ogni evento o serie di eventi collegati, non pianificati dalla intermediario, che ha, o che potrebbe avere, un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi di pagamento”.

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 processo in oggetto, tali eventi vengono 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 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'intermediario¹.
- 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 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.

¹ 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.

- 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.
- 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

Il prestatore di servizio di pagamento (PSP) segnala tutti i “gravi” incidenti operativi o di sicurezza, a prescindere dal fatto che si verifichino presso succursali o affiliate all'interno o al di fuori dell'Italia, all'interno o al di fuori dell'area dell'euro².

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

- il rapporto iniziale relativo all'incidente, atteso entro quattro ore dalla prima rilevazione di un “grave” incidente operativo o di sicurezza.

Il PSP include nel rapporto iniziale 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. Il PSP ricorre a stime quando non sono disponibili i dati effettivi. Il PSP 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 rapporti intermedi attesi entro 3 giorni lavorativi dall'invio del precedente rapporto (iniziale o precedente rapporto intermedio).

Il PSP invia un rapporto intermedio ogniqualvolta ritenga che vi sia un aggiornamento rilevante dello stato dell'incidente e comunque entro la data del successivo aggiornamento indicata nel rapporto precedente (rapporto iniziale o precedente rapporto intermedio).

Il PSP sottomette il primo rapporto intermedio con una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione in blu del modulo). Inoltre, il PSP fornisce ulteriori rapporti intermedi 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

² 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 riguarda ad esempio i servizi 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).

identificate o azioni intraprese per risolvere il problema). In ogni caso, il PSP presenta un rapporto intermedio quando esplicitamente richiesto dalla Banca d'Italia.

Come nel caso dei rapporti iniziali, qualora dati effettivi non siano disponibili, il PSP può ricorrere a stime.

Inoltre, il PSP 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, il PSP 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 intermedio, aggiornando esclusivamente le informazioni relative alla data stimata per l'aggiornamento successivo.

Il PSP invia l'ultimo rapporto intermedio 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 dal PSP 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.

Se l'attività dovesse ritornare alla normalità prima che siano trascorse quattro ore dalla rilevazione dell'incidente "grave", il PSP deve adoperarsi per presentare simultaneamente sia il rapporto iniziale sia l'ultimo rapporto intermedio (ossia compilando le sezioni rossa e blu del modulo) entro le quattro ore previste per l'invio del rapporto iniziale.

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

Il rapporto finale deve essere inviato una volta avviata l'analisi delle cause che hanno originato l'incidente (indipendentemente dal fatto che siano state già attuate misure di mitigazione o che sia stata individuata definitivamente la causa che ha originato l'incidente) e quando sono disponibili dati effettivi da sostituire alle eventuali stime effettuate. Nel rapporto 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 rapporto finale non includa tutte le informazioni necessarie perché non disponibili nei tempi richiesti (due settimane dalla chiusura dell'incidente), al PSP sarà richiesto di inviare una relazione di chiusura, eventualmente nel formato standard del rapporto finale o libero a seconda dei casi.

È sempre possibile anticipare la compilazione di campi relativi ad un rapporto successivo se si possiede l'informazione e modificare campi già compilati in un rapporto precedente se necessario.

Il modulo da utilizzare per i suddetti rapporti, disponibile sia in versione italiana che inglese, è annesso alle presenti istruzioni (cfr. documento “comunicazione_incidenti_IPIMEL_2019_ITA(ENG).pdf”). Il PSP, laddove lo ritenga necessario, può integrare il modulo standardizzato con documentazione integrativa, sotto forma di uno o più allegati.

Ogni rapporto 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_32 – WWWWW XXXXX YYYYY”, “”, dove WWWWW va valorizzato con “PRIMO”, “INTERMEDIO”, “FINALE”, “RELAZIONE” (nel caso di relazione successiva al rapporto finale) con riguardo al rapporto allegato, mentre XXXXX e YYYYY rappresentano rispettivamente il codice ABI e il nome dell'intermediario 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 il PSP nel caso di inoltro dei rapporti all'Autorità bancaria europea.

I PSP devono inoltre presentare al nostro Istituto, se applicabile, una copia delle comunicazioni che sono state effettuate (o saranno effettuate) ai propri utenti, come previsto dall'articolo 96, paragrafo 1, comma 2, della PSD2, non appena disponibili.

3. Criteri e soglie per la segnalazione

I PSP classificano come “gravi”, e quindi li segnalano, gli incidenti operativi o di sicurezza che soddisfano

- a. uno o più criteri al «livello di impatto maggiore», o
- b. tre o più criteri al «livello di impatto minore»

I criteri sono indicati nella Tabella 1, distinguendo tra quelli “di impatto minore” e quelli “di impatto maggiore” e seguendo i criteri di valutazione dei criteri indicati nel seguito di questa sezione.

Criteri	Livello di impatto minore	Livello di impatto maggiore
1) Transazioni interessate	> 10 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) e > 100 000 EUR	> 25 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) o > 5 milioni di EUR
2) Utenti di servizi di pagamento interessati	> 5 000 e > 10 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento	> 50 000 o > 25 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento
3) Periodo di indisponibilità del servizio	> 2 ore	Non applicabile
4) Impatto economico	Non applicabile	> Max (0,1 % capitale di tipo "Tier 1" ³ , 200 000 EUR) o > 5 milioni di EUR
5) Alto livello di escalation interna	Sì	Sì e probabilmente si ricorrerà alla modalità di crisi aziendale (o equivalente)
6) Altri PSP o infrastrutture connesse potenzialmente coinvolti	Sì	Non applicabile
7) Impatto sulla reputazione	Sì	Non applicabile

Tabella 1: Criteri per la classificazione di incidenti operativi o di sicurezza "gravi"

I PSP devono basare la propria valutazione di gravità di un incidente operativo o di sicurezza sui seguenti criteri e sui rispettivi indicatori sottostanti.

1) Transazioni interessate

I PSP determinano 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, i PSP considerano 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, i PSP devono 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 i PSP non ritengono che tale dato sia rappresentativo (ad esempio, a causa della stagionalità), essi possono utilizzare un'altra metrica, più rappresentativa, e comunicare la motivazione alla base di tale approccio compilando il campo corrispondente del modulo.

³ Capitale di tipo "Tier 1", come definito nell'articolo 25 del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012.

2) Utenti del servizio di pagamento interessati

I PSP determinano il numero di utenti del servizio di pagamento interessati, sia in termini assoluti sia in percentuale del numero totale di utenti del servizio di pagamento.

I PSP considerano come «utenti del servizio di pagamento interessati» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con il PSP interessato che garantisce loro l'accesso al servizio di pagamento interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. I PSP devono ricorrere a stime basate su dati storici per determinare il numero di utenti del servizio di pagamento che potrebbero aver utilizzato tale servizio nel corso dell'incidente.

Nel caso di un PSP che offre servizi operativi a terzi, tale PSP deve considerare solo i propri utenti dei servizi di pagamento (se ve ne sono). Similmente, i PSP che ricevono servizi operativi da altri PSP devono valutare l'incidente in relazione ai soli propri utenti dei servizi di pagamento.

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

3) Periodo di indisponibilità del servizio

I PSP determinano 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 dal PSP.

I PSP considerano 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. I PSP calcolano il periodo di indisponibilità del servizio dal momento del suo inizio e considerano 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 i PSP non sono in grado di determinare il momento di inizio del periodo di inattività del servizio, essi possono eccezionalmente calcolare tale periodo a partire dal momento in cui l'indisponibilità è stata rilevata.

4) Impatto economico

I PSP determinano in modo olistico i costi monetari associati all'incidente per tenere conto sia della cifra assoluta sia, se applicabile, dell'importanza relativa di tali costi in relazione alla dimensione del prestatore di servizi di pagamento (ossia al capitale di tipo Tier 1 del prestatore di servizi di pagamento).

I PSP considerano sia i costi che possono essere collegati direttamente all'incidente sia quelli che sono indirettamente associati ad esso. Tra le altre cose, i PSP devono tener conto dei fondi o dei beni espropriati, dei costi di sostituzione dell'hardware o del software, di altri costi di indagine o di riconfigurazione, delle penali dovute alla mancata osservanza di obblighi contrattuali, delle sanzioni, delle passività esterne e delle perdite di entrate. Per quanto riguarda i costi indiretti, i PSP devono considerare solo quelli già noti o molto probabili.

5) Alto livello di escalation interna

I PSP determinano se l'incidente è stato o sarà probabilmente segnalato ai rispettivi dirigenti esecutivi.

I PSP considerano se, in conseguenza dell'impatto dell'incidente sui servizi connessi ai pagamenti, il responsabile della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell'accaduto in via straordinaria rispetto alla procedura di informazione periodica e in modo continuativo per tutta la durata dell'incidente. Inoltre, i PSP considerano se, a seguito dell'impatto dell'incidente sui servizi connessi ai pagamenti, è stata o sarà probabilmente attivata la modalità di crisi aziendale.

6) Altri PSP, operatori o infrastrutture connesse potenzialmente coinvolti

I PSP determinano le implicazioni sistemiche che l'incidente probabilmente avrà, ossia il suo potenziale di estendersi oltre il PSP inizialmente interessato ad altri prestatori di servizi di pagamento, infrastrutture dei mercati finanziari e/o a schemi di carte di pagamento.

I PSP valutano l'impatto dell'incidente sui mercati finanziari, inteso come infrastrutture dei mercati finanziari e/o schemi di pagamento con carte che li supportano e altri prestatori di servizi di pagamento. In particolare, i PSP valutano se l'incidente si è ripetuto o probabilmente si ripeterà presso altri prestatori di servizi di pagamento, se ha influenzato o probabilmente influenzerà il buon funzionamento delle infrastrutture dei mercati finanziari e se ha compromesso o probabilmente comprometterà il regolare funzionamento del sistema finanziario nel suo complesso. I PSP devono tener conto di vari elementi, ad esempio se il componente/software interessato è proprietario o genericamente disponibile, se la rete compromessa è interna o esterna e se il prestatore di servizi di pagamento ha smesso o probabilmente smetterà di adempiere i propri obblighi nelle infrastrutture del mercato finanziario di cui è membro.

7) Impatto sulla reputazione

I PSP determinano in che modo l'incidente possa minare la fiducia degli utenti nei confronti del PSP stesso e, più in generale, nei confronti dei servizi coinvolti o del mercato nel suo complesso.

I PSP considerano il livello di visibilità che, per quanto di loro conoscenza, l'incidente ha ricevuto o probabilmente riceverà sul mercato. In particolare, i PSP devono considerare la probabilità che l'incidente causi danni alla società quale valido indicatore del suo potenziale di influenzare la loro reputazione. I PSP considerano se (i) 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.), (ii) non si sono adempiuti o probabilmente non si adempiranno obblighi regolamentari, (iii) sono state o probabilmente saranno violate sanzioni o (iv) lo stesso tipo di incidente si è già verificato in passato.

4. Il modello per la segnalazione degli incidenti di sicurezza informatica

I PSP devono utilizzare il modello standardizzato in formato PDF (cfr. documento in italiano o in inglese, a seconda della convenienza del PSP, “comunicazione_incidenti_IPIMEL_2019_ITA(ENG).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 rapporto finale. Qualora il PSP lo desideri, assieme al modello, è possibile fornire documentazione aggiuntiva, come le prove relative dell'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 rapporto iniziale (campi rossi);
- campi obbligatori per i rapporti intermedi (campi azzurri);
- campi obbligatori per il rapporto 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 rapporto successivo se si possiede l'informazione e modificare campi già compilati in un rapporto precedente se necessario.

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

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

Rapporto iniziale: il primo rapporto relativo all'incidente, atteso entro quattro ore dal momento della rilevazione

Rapporto intermedio: i successivi rapporti relativi all'incidente (rapporto intermedio), attesi entro 3 giorni lavorativi dall'invio del rapporto iniziale o dei precedenti rapporti intermedi)

Ultimo rapporto intermedio: ultimo rapporto intermedio, da inviare dopo che la l'attività è tornata alla normalità

Rapporto finale: rapporto finale relativo all'incidente, atteso entro 2 settimane dalla chiusura dell'incidente (utilizzare questo campo anche in caso di relazione di chiusura)

Data e ora del rapporto: data e ora di compilazione del rapporto

Numero di identificazione dell'incidente (solo per rapporti intermedi o finali): identificativo dell'incidente, fornito da Banca d'Italia dopo l'invio del rapporto iniziale, da inserire nei corrispondenti rapporti successivi (intermedio e finale).

Quando è previsto il prossimo aggiornamento?: indicare data e ora stimate per la presentazione dell'aggiornamento successivo (rapporto intermedio, finale, relazione conclusiva)

Prossimo aggiornamento - motivazione: indicare, se necessario, le ragioni della tempistica proposta per l'aggiornamento successivo

Incidente riclassificato come non grave: selezionare nei rapporti successivi al primo, se ad un'analisi più approfondita la classificazione dell'incidente è stata ridotta a "non grave" e motivare.

Campi rossi – Rapporto iniziale

- *Nome dell'istituto:* nome dell'ente segnalante
- *Codice ABI:* codice ABI dell'ente segnalante
- *Numero di iscrizione all'Albo:* numero di iscrizione all'Albo dell'ente segnalante
- *Paese o paesi interessati dall'incidente* (ad esempio, sono interessate diverse succursali del gruppo situate in vari Stati).
- *Primo e secondo referente all'interno del PSP:* 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 rapporti intermedio 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.
- *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 rapporto iniziale. L'importanza di un incidente rilevato, ad esempio, può aumentare nel tempo o l'entità del problema può manifestarsi soltanto in un secondo momento.
- *L'incidente è stato rilevato da:* si deve indicare chi per primo ha segnalato l'incidente.
- *Tipo di incidente:* selezionare l'opzione incidente "Attacco cyber" o "Incidente operativo", una volta accertata la natura dell'incidente. Se al momento della compilazione del rapporto non è chiaro se l'incidente sia dovuto ad un attacco, selezionare "sconosciuto".
- *Descrizione generale dell'incidente:* è il campo in cui inserire le informazioni relative all'incidente grave note al momento dell'invio del rapporto iniziale. È possibile rivedere e/o migliorare la descrizione sintetica all'invio dei rapporti intermedio e finale (sono predisposti campi distinti).

Campi azzurri – Rapporto intermedio

- *Data e ora di inizio dell'incidente (se già nota)*: data e ora in cui l'incidente è iniziato, se noto.
- *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.
- *L'incidente è 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 rapporti intermedi e finale.
- *Descrizione dettagliata dell'incidente*: fornire informazioni dettagliate relative all'incidente grave e note al momento dell'invio del rapporto intermedio. È possibile rivedere e/o migliorare la descrizione all'invio del rapporto finale.

Informazioni sull'incidente

- *L'incidente vi ha interessati direttamente o attraverso un fornitore di servizi?*: 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 questo ultimo caso, il nome del/dei fornitori.
- 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 di sicurezza informatica 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 il PSP non attenendosi intenzionalmente alle policy di sicurezza e di diritto di accesso.
 - 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.
- Tipo di incidente, nel caso incidenti operativi:

- *Eventi accidentali*: incidenti causati da eventi accidentali, come ad esempio errori umani (fa eccezione la diffusione/alterazione di dati accidentale, classificata in questo contesto come cyber)
- *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).
- *Problema software*: incidenti dovuti al malfunzionamento di programmi software applicativi o di base;
- *Problema hardware o infrastrutturale*: incidenti dovuti a malfunzionamenti di sistemi e componenti hardware ovvero di reti di comunicazione o piattaforme condivise.
- *Sabotaggio*: sabotaggio di apparati tramite accesso fisico
- *Evento naturale*: incidenti causati da cause naturali o esterne, come inondazioni, incendi, terremoti.
- *Se altro, specificare*

Classificazione e impatto dell'incidente

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

- *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.
- *Transazioni interessate*: 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).

- *Utenti di servizi di pagamento interessati*: indicare il numero totale di utenti di servizi di pagamento che sono stati interessati e la percentuale di utenti di servizi di pagamento interessati rispetto al numero totale di utenti di servizi di pagamento. 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).
- *Periodo di indisponibilità del servizio*: PSP devono indicare se la soglia è stata o probabilmente sarà raggiunta dall’incidente e i dati relativi: periodo totale di indisponibilità del servizio. Per questa variabile, i PSP 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).
- *Impatto economico*: PSP devono indicare se la soglia è stata o probabilmente sarà raggiunta dall’incidente e i dati relativi. Per questa variabile, i PSP 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).
- *Alto livello di escalation interna*: i PSP devono considerare se, in conseguenza dell’impatto dell’incidente sui servizi connessi ai pagamenti, il responsabile della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell’accaduto in via straordinaria rispetto alla procedura di informazione periodica e in modo continuativo per tutta la durata dell’incidente (si faccia riferimento alla sezione “Criteri e soglie per la segnalazione” per maggiori dettagli).
- *Altri intermediari, operatori o infrastrutture rilevanti coinvolti o potenzialmente interessati (impatto sistemico)*: i PSP devono valutare l’impatto dell’incidente sui mercati finanziari, inteso come infrastrutture dei mercati finanziari e/o schemi di pagamento con carte che li supportano e altri prestatori di servizi di pagamento (si faccia riferimento alla sezione “Criteri e soglie per la segnalazione” per maggiori dettagli).
- *Possibili violazioni di obblighi legali o regolamentari*: indicare se l’incidente implica o possa implicare violazioni di obblighi legali o regolamentari.
- *Impatto sulla reputazione*: prestatori di servizi di pagamento dovrebbero considerare il livello di visibilità che, per quanto di loro conoscenza, l’incidente ha ricevuto o probabilmente riceverà sul mercato (si faccia riferimento alla sezione “Criteri e soglie per la segnalazione” per maggiori dettagli).
- *Altri impatti (se presenti, specificare)*: specificare se necessario altri impatti non rientranti nelle categorie sopra indicate.

Dettagli sull’impatto dell’incidente

- *Edificio/i interessato/i (indirizzo), se applicabile (se presenti, specificare)*: se è interessato un edificio fisico, indicarne l’indirizzo.

- *Sistemi e componenti interessati*: selezionare uno o più degli elementi forniti nel modello.
- *Canali commerciali interessati*: selezionare uno o più degli elementi forniti nel modello.
- *Servizi di pagamento interessati*: selezionare uno o più degli elementi forniti nel modello.
- *Aree funzionali dei servizi di pagamento interessati*: selezionare uno o più degli elementi forniti nel modello.
- *Personale interessato*: indicare se l'incidente ha avuto effetti sul personale e, in caso affermativo, fornire dettagli nel campo di testo libero.

Analisi, misure di mitigazione e risoluzione dell'incidente

- *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.
- *E' stato attivato il piano di continuità operativa e/o il piano di disaster recovery? In caso affermativo, quando, come?*: si veda la sezione "Criteri e soglie per la segnalazione" per maggiori dettagli.
- *Il PSP ha annullato o attenuato 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 - Segnalazione definitiva

- *Descrizione dettagliata*: fornire informazioni dettagliate relative all'incidente grave e note al momento dell'invio del rapporto definitivo. Si devono aggiungere informazioni più approfondite sull'incidente, aggiornando quelle fornite nel corrispondente campo del rapporto intermedio, nonché un'accurata analisi delle cause. Il modello suggerisce una serie di dettagli da fornire. Si deve, tuttavia, riportare qualsiasi dettaglio disponibile.

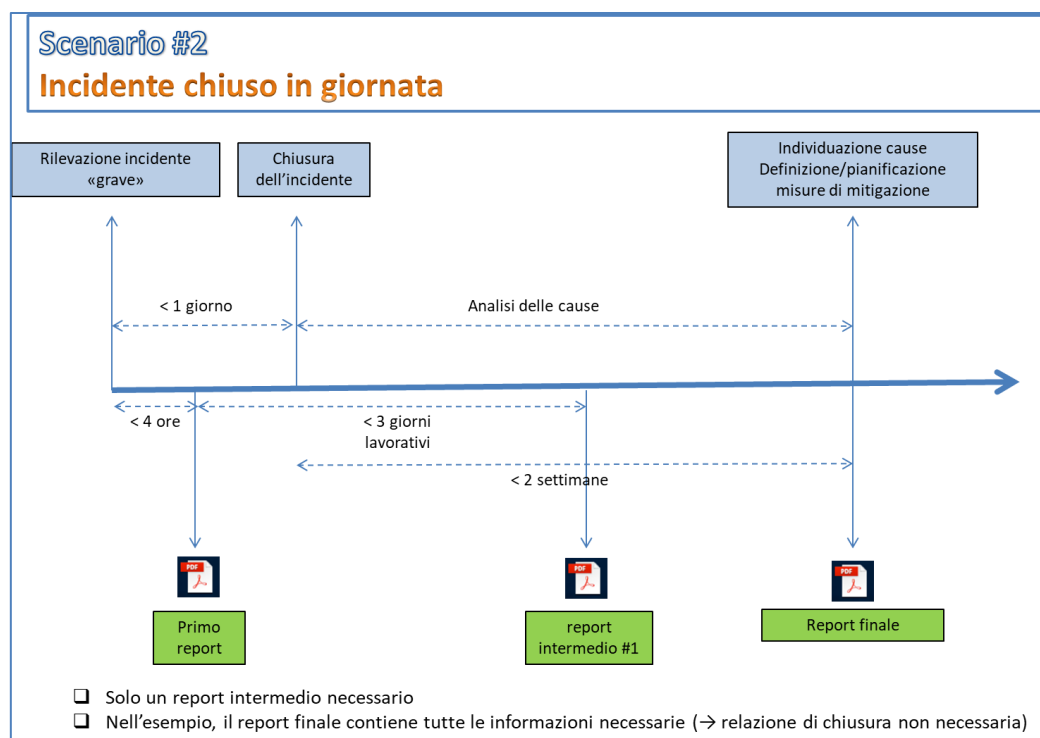
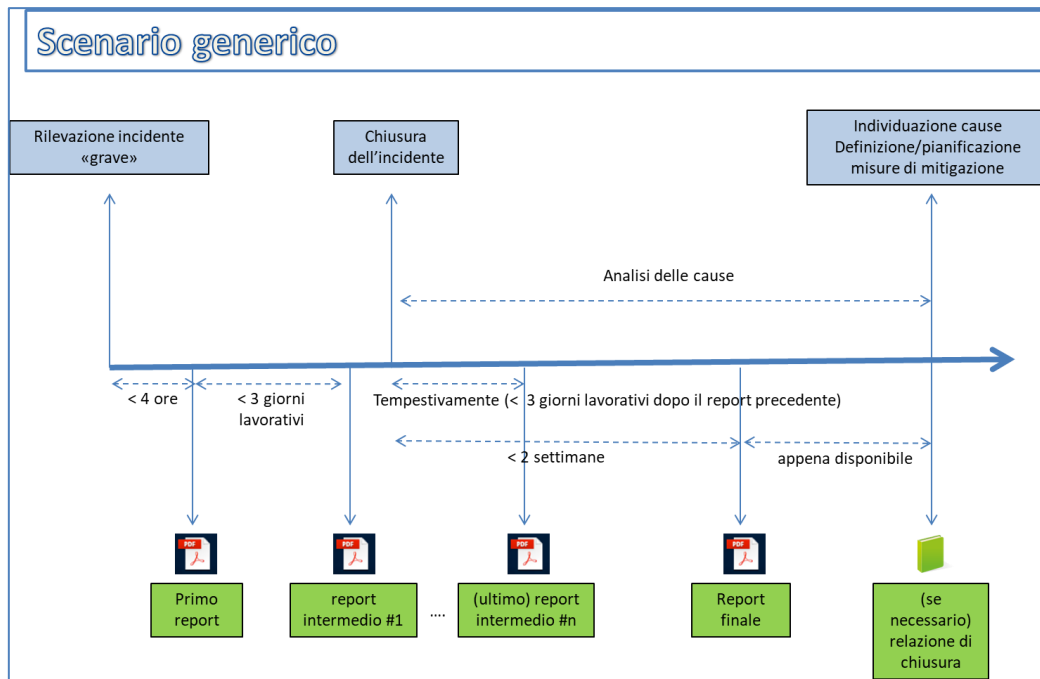
Analisi, misure di mitigazione e risoluzione dell'incidente

- *Le misure di controllo originali sono state 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.
- *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.

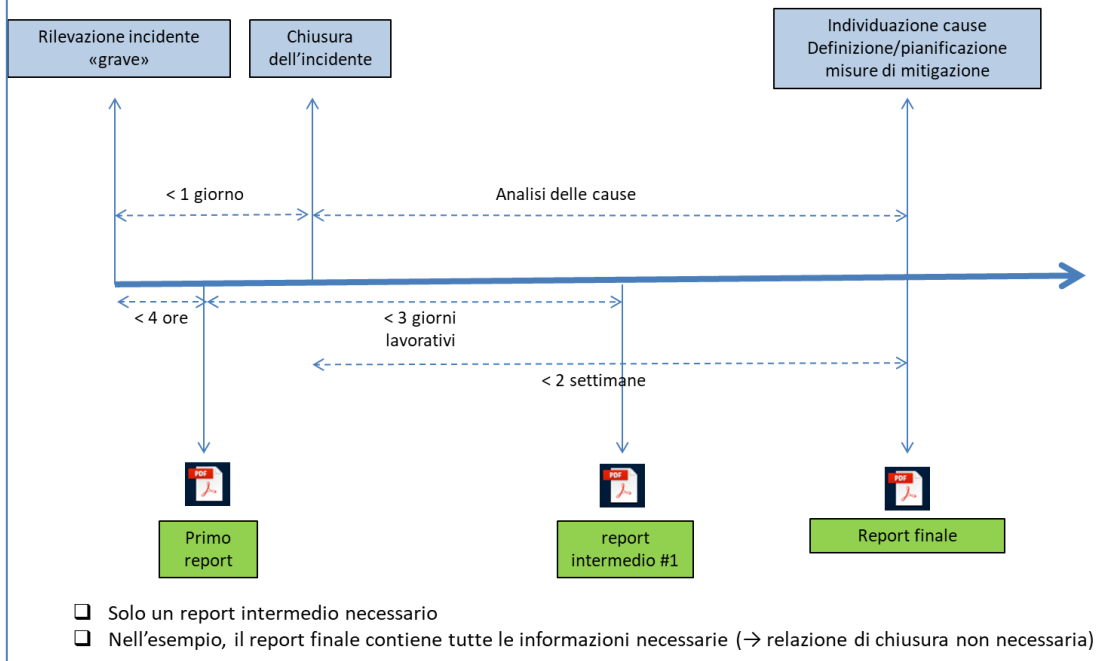
- *Principali azioni correttive/misure adottate o pianificate per impedire che l'incidente si verifichi nuovamente in futuro, se già note:* descrivere le principali azioni intraprese o previste per evitare il ripetersi dell'incidente in futuro.
- *L'incidente è stato segnalato al CERT/CSIRT nazionale?*
- *Le informazioni sull'incidente sono state condivise con altri intermediari finanziari? E al CertFIN?*
- *Sono state intraprese azioni legali contro il gruppo o entità del gruppo?*

ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione



Scenario #2

Incidente chiuso in giornata



Scenario #3

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

