ISTRUZIONI PER LA SEGNALAZIONE DEI GRAVI INCIDENTI OPERATIVI O DI SICUREZZA[1]– BANCHE LESS SIGNIFICANT E SUCCURSALI DI BANCHE EXTRA-COMUNITARIE[2]

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

Indice

1. Definizioni

1.1. Ai sensi della Circ. n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, Tit. IV, Cap. 4, Sez. 1, Par. 3), con "incidente operativo o di sicurezza" si intende "ogni evento, o serie di eventi collegati, non pianificati dalla banca che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull'integrità, la disponibilità, la riservatezza e/o l'autenticità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi)";

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

[2] Banche extra-comunitarie ad eccezione di quelle aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive della Circolare n.285

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 disposizioni per la gestione degli incidenti operativi o di sicurezza anche alla gestione degli incidenti operativi relativi alla prestazione dei servizi di pagamento anche se 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)).

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

- Incidenti cyber: incidenti causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzati delle risorse della banca o incidenti che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario.
- Incidenti operativi: incidenti derivanti da processi inadeguati o malfunzionanti, persone e sistemi o eventi di forza maggiore. Tra tali eventi sono inclusi quelli naturali, errori

software/hardware, eventi accidentali, malfunzionamenti di processo, sabotaggio (attacco fisico). La diffusione e/o l'alterazione involontaria (ad esempio, per errore umano o software) di dati riservati della clientela e/o dell'intermediario ricade nella categoria degli incidenti cyber.

Di seguito infine alcune definizioni di termini adottati nel documento:

- Integrità: Proprietà della salvaguardia dell'esattezza e completezza delle risorse (inclusi i dati).
- Disponibilità: Proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento.
- Riservatezza: Proprietà per cui le informazioni non sono rese disponibili o divulgate a persone, entità o procedure non autorizzate.
- Autenticità: Proprietà di una fonte di essere quella che dichiara di essere.
- Servizi connessi ai pagamenti: Attività commerciali definite nell'articolo 4, paragrafo 3, della PSD2 e tutte le attività di supporto tecnico necessarie per la corretta fornitura dei servizi di pagamento.

2. Modalità di segnalazione

La banca (la capogruppo nel caso di gruppi bancari), segnala tutti i "gravi" incidenti operativi o di sicurezza e gli incidenti operativi relativi alla prestazione dei servizi di pagamento anche se non collegati al funzionamento delle risorse e dei processi ICT (entrambi di seguito indicati come incidenti), a prescindere dal fatto che si verifichino presso succursali o affiliate all'interno o al di fuori dell'Italia[3].

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

- il rapporto iniziale relativo all'incidente, atteso entro quattro ore dal momento in cui l'incidente è stato classificato come "grave" secondo i criteri descritti nella sezione 3.

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

  L'intermediario 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

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

conseguenze previste sulla base delle informazioni disponibili subito dopo che è stato rilevato e classificato come grave. L'intermediario ricorre a stime quando non sono disponibili i dati effettivi.

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

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

- il rapporto intermedio, inviato quando le regolari operazioni sono state ripristinate e l'attività è tornata alla normalità (chiusura dell'incidente[4]). Se le normali attività non sono state ancora ripristinate, il rapporto intermedio va trasmesso comunque entro tre giorni lavorativi dalla trasmissione del rapporto iniziale.

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

  L'intermediario sottomette il rapporto intermedio con una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione in blu del modulo). Inoltre, l'intermediario fornisce gli ulteriori eventuali rapporti intermedi aggiornando le informazioni già inserite nelle sezioni rossa e blu del modulo. In ogni caso, l'intermediario presenta un rapporto intermedio 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.

  Se l'attività dovesse ritornare alla normalità prima che siano trascorse quattro ore dal momento della classificazione dell'incidente come "grave", l'intermediario deve adoperarsi per presentare simultaneamente sia il rapporto iniziale sia il 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 20 giorni lavorativi dalla chiusura dell'incidente (momento in cui si considera che le attività siano tornate alla normalità).

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

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

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

Nel caso di chiusura del grave incidente entro le quattro ore dal momento della sua classificazione, laddove l'intermediario sia in grado di fornire tutte le informazioni richieste dal rapporto intermedio e dal rapporto finale, esso dovrebbe adoperarsi per fornire congiuntamente le informazioni relative al rapporto iniziale, intermedio e finale (ossia compilare le sezioni rossa, blu e verde del modulo).

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

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

Il modulo da utilizzare per i suddetti rapporti, disponibile sia in versione italiana che inglese, è annesso alle presenti istruzioni (cfr. documento "comunicazione_incidenti_LSI_2021_ITA(ENG).pdf"). Gli intermediari, laddove ritenuto necessario, possono integrare il modulo standardizzato con documentazione integrativa, sotto forma di uno o più allegati. Per la compilazione dei campi presenti nel modulo, gli intermediari seguono le istruzioni contenute nel presente documento.

Ogni rapporto (e gli eventuali documenti allegati) dovrà essere allegato ad un messaggio di posta elettronica certificata e inviato alla casella di PEC Supervisione_rischio_ICT@pec.bancaditalia.it**;** l'oggetto del messaggio dovrà indicare il rapporto allegato, il tipo di incidente segnalato e l'ente segnalante, secondo il seguente schema: "Oggetto: Com_incidente – 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 della banca segnalante.

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

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

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 rapporti alla Banca centrale europea e/o all'Autorità bancaria europea.

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

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

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

3. Criteri e soglie per la segnalazione

Gli intermediari classificano come "gravi", e quindi li segnalano, gli incidenti 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 (solo per servizi di pagamento)	> 10% del livello normale delle transazioni (in termini di numero di transazioni) e durata dell'incidente > 1 ora* o > 500 000 EUR e durata dell'incidente > 1 ora*	> 25 % del livello normale delle transazioni (in termini di numero di transazioni) o > 15 000 000 EUR
2) Utenti interessati	> 5000 e durata dell'incidente > 1 ora* o	> 50 000 **o** > 25 % degli utenti del/i servizio/i interessato/i dall'incidente

	> 10 % degli utenti del/i servizio/i interessato/i dall'incidente e durata dell'incidente > 1 ora*	
3) Periodo di indisponibilità del servizio	> 2 ore	Non applicabile
4) Impatto economico	Non applicabile	> Max (0,1 % capitale di tipo "Tier 1"[5], 200 000 EUR) **o** > 5 milioni di EUR
5) Violazione della sicurezza della rete o dei sistemi informativi	SI	Non applicabile
6) Alto livello di escalation interna	Sì	Sì e probabilmente si ricorrerà alla modalità di crisi aziendale (o equivalente)
7) Altri intermediari o infrastrutture rilevanti potenzialmente coinvolti	Sì	Non applicabile
8) Impatto sulla reputazione	Sì	Non applicabile

* La soglia relativa alla durata dell'incidente per un periodo superiore a un'ora si applica solo agli incidenti operativi che incidono sulla capacità del prestatore di servizi di pagamento di iniziare e/o elaborare transazioni.

Tabella 1: Criteri per la classificazione di incidenti "gravi"

Nel caso di gruppi bancari, i criteri e le soglie vanno considerati a livello consolidato nel caso l'incidente interessi il gruppo nel suo insieme (ad esempio, un incidente che colpisca i sistemi informativi della capogruppo e che abbia effetti sulle entità più rilevanti del gruppo), ovvero a livello di singola entità nel caso l'incidente sia limitato ad una o più entità del gruppo (ad esempio, l'incidente interessi i sistemi informativi gestiti e utilizzati da una singola entità del gruppo).

Gli intermediari devono basare la propria valutazione di gravità di un incidente sui seguenti criteri e sui rispettivi indicatori sottostanti:

1) <u>Transazioni interessate (nel caso l'incidente interessi servizi di pagamento)</u>

Gli intermediari 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, gli intermediari 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

[5] 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.

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).

Per gli incidenti operativi che incidono sulla capacità di iniziare e/o elaborare transazioni, gli intermediari dovrebbero segnalare solo gli incidenti che hanno una durata superiore a un'ora. La durata dell'incidente dovrebbe essere misurata dal momento in cui l'incidente si verifica al momento in cui le normali attività/operazioni sono state ripristinate al livello di servizio prestato prima dell'incidente.

Inoltre, gli intermediari 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 gli intermediari 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.

2) <u>Utenti interessati</u>

Gli intermediari determinano il numero di utenti del servizio colpito dall'incidente interessati, sia in termini assoluti sia in percentuale del numero totale di utenti del servizio.

Gli intermediari considerano come «utenti del servizio interessati» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con l'intermediario e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. Gli intermediari devono ricorrere a stime basate sull'attività precedente per determinare il numero di utenti del servizio che potrebbero aver utilizzato il servizio nel corso dell'incidente.

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

Per gli incidenti operativi con impatto sui servizi di pagamento e che incidono sulla capacità di iniziare e/o elaborare transazioni, gli intermediari dovrebbero segnalare solo gli incidenti che hanno una durata superiore a un'ora. La durata dell'incidente dovrebbe essere misurata dal momento in cui l'incidente si verifica al momento in cui le normali attività/operazioni sono state ripristinate al livello di servizio prestato prima dell'incidente.

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

3) <u>Periodo di indisponibilità del servizio di pagamento</u>

Gli intermediari determinano il periodo di tempo in cui il servizio interessato dall'incidente 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.

Gli intermediari 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. Gli intermediari calcolano il periodo di indisponibilità del servizio dal momento del suo inizio e considerano sia gli intervalli di tempo in cui sono operativi sia gli orari di chiusura e i periodi di manutenzione, se del caso e se applicabile. Se gli intermediari 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

Gli intermediari determinano in modo olistico i costi monetari associati all'incidente e tengono conto sia della cifra assoluta sia, se applicabile, dell'importanza relativa di tali costi in relazione alla dimensione dell'intermediario (ossia al capitale di tipo Tier 1 dell'intermediario).

Gli intermediari considerano sia i costi che possono essere collegati direttamente all'incidente sia quelli che sono indirettamente associati ad esso. Tra le altre cose, gli intermediari 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, gli intermediari devono considerare solo quelli già noti o molto probabili.

5) Violazione della sicurezza della rete o dei sistemi informativi

Gli intermediari determinano se un'azione dolosa ha compromesso la disponibilità, l'autenticità, l'integrità o la riservatezza della rete o dei sistemi informativi (inclusi i dati) dell'intermediario.

6) Alto livello di escalation interna

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

Gli intermediari 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, gli intermediari considerano se, a seguito dell'impatto dell'incidente sui servizi connessi ai pagamenti, è stata o sarà probabilmente attivata la modalità di crisi aziendale.

7) Altri intermediari o infrastrutture rilevanti potenzialmente coinvolti

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

Gli intermediari 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, gli intermediari 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. Gli intermediari 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 l'intermediario ha smesso o probabilmente smetterà di adempiere i propri obblighi nelle infrastrutture del mercato finanziario di cui è membro.

8) Impatto sulla reputazione

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

Gli intermediari considerano il livello di visibilità che, per quanto di loro conoscenza, l'incidente ha ricevuto o probabilmente riceverà sul mercato. In particolare, gli intermediari devono considerare la probabilità che l'incidente causi danni alla società quale valido indicatore del suo potenziale di influenzare la loro reputazione. Gli intermediari considerano se (i) gli utenti di servizi di pagamento e/o altri prestatori di servizi di pagamento si sono lamentati dell'impatto negativo dell'incidente , (ii) l'incidente ha influito su un processo visibile e pertanto riceverà probabilmente o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i giornali, ma anche blog, social networks, ecc.), (iii) sono stati o saranno probabilmente disattesi obblighi contrattuali, con la conseguente pubblicazione di azioni legali contro il prestatore di servizi di pagamento (iv) non si sono adempiuti obblighi regolamentari con la conseguente imposizione di misure di vigilanza o sanzioni che sono state o saranno probabilmente rese pubbliche o, (v) lo stesso tipo di incidente si è già verificato in passato.

Se sulla base dei precedenti criteri l'intermediario stabilisce che l'incidente non è grave, ha tuttavia la possibilità di considerarlo tale secondo criteri definiti internamente. Più precisamente, l'intermediario può comunque segnalare l'incidente alla Banca d'Italia nel caso in cui individui un'importante interruzione dei servizi, un danno reputazionale, un impatto legale o regolamentare, uno svantaggio competitivo o un potenziale impatto sistemico.

Se la valutazione della rilevanza non conduce a un risultato chiaro (ad esempio non è chiaramente distinguibile il perimetro dell'incidente, le entità coinvolte e le corrispondenti soglie relative ai criteri di rilevanza), l'incidente è da considerarsi grave.

Qualora diversi incidenti appaiano tra loro collegati, l'intermediario deve avvalersi delle valutazioni dei propri esperti per decidere se tali eventi determinino un unico incidente o corrispondano a più incidenti.

Nel caso di gruppi bancari, se la segnalazione di un incidente interessa 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; (ii) utilizzando intervalli di valori, nei campi dove ciò è consentito, indicando il valore più basso e quello più alto osservati o stimati per le diverse entità.

4. Il modello per la segnalazione degli incidenti

Gli intermediari devono utilizzare il modello standardizzato in formato PDF (cfr. documento in italiano o in inglese, a seconda della convenienza dell'intermediario, "comunicazione_incidenti_LSI_2021_ITA(ENG).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 rapporto finale. Qualora l'intermediario lo desideri, assieme al modello è possibile fornire documentazione aggiuntiva, come le prove relative all'attacco o la documentazione dell'infrastruttura per la sicurezza oltre che la copia delle eventuali comunicazioni che sono state effettuate (o saranno effettuate) ai propri clienti, come previsto dall'articolo 96, paragrafo 1, comma 2, della PSD2.

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

- campi obbligatori per il rapporto iniziale (campi rossi);
- campi obbligatori per il rapporto intermedio (campi blu);
- 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.

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

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

Intestazione

*Rapporto iniziale***:** il rapporto iniziale relativo all'incidente, atteso entro quattro ore dal momento in cui esso è stato classificato come "grave".

Rapporto intermedio: il rapporto da inviare dopo che l'attività è tornata alla normalità ma in ogni caso non oltre tre giorni lavorativi dopo il rapporto iniziale.

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

*Data e ora del rapporto***:** data e ora di trasmissione del rapporto

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

Modifiche apportate ai rapporti precedenti: indicare le modifiche apportate alle informazioni già fornite con i rapporti precedenti (es. il rapporto iniziale o, ove applicabile, il rapporto intermedio).

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", indicando eventualmente una motivazione nel campo "*Riclassificato come non grave - motivazione*".

Rapporto iniziale - Campi rossi

Informazioni generali

- *Codice ABI dell'istituto segnalante*: codice ABI dell'ente segnalante
- *Nome dell'istituto segnalante:* nome dell'ente segnalante
  Referente principale e secondario da contattare: 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.
- *Paese o paesi interessati dall'incidente*: paese o paesi in cui si è verificato l'incidente

Rilevamento e classificazione incidente

- *Data e ora di rilevazione dell'incidente*: la data e ora in cui l'incidente è stato rilevato per la prima volta. La data non deve necessariamente coincidere con la data del 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.
- *Data e ora di classificazione dell'incidente*: la data e ora in cui l'incidente è stato classificato come grave. Nel caso in cui il rapporto iniziale venga trasmesso in ritardo (oltre le 4 ore dalla

classificazione come incidente grave) i motivi di tale ritardo devono essere riportati nel campo "*Motivi per invio ritardato rapporto iniziale".*

- *L'incidente è stato rilevato da*: si deve indicare chi per primo ha rilevato l'incidente.
- *Tipo di incidente*: selezionare l'opzione incidente "cyber" o "*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".
- *L'incidente interessa servizi di pagamento ?*: indicare se l'incidente ha impatti su servizi di pagamento offerti dall'intermediario ai propri clienti.
- *Motivo/i 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.
- *Impatti in altri Stati membri UE, se applicabile*: indicare gli eventuali impatti che l'incidente ha avuto in un altro/i Stato/i membro/i dell'UE (ad esempio su utenti, altri intermediari e/o infrastrutture di pagamento).
- *Segnalazione ad altre autorità*: indicare se l'incidente è stato/sarà segnalato ad altre autorità, se noti al momento della segnalazione. In caso affermativo, specificare le predette autorità.
- *Una breve e generale descrizione dell'incidente*: è il campo in cui inserire le informazioni relative all'incidente grave note al momento dell'invio del rapporto iniziale. È possibile rivedere e/o migliorare la descrizione sintetica all'invio dei rapporti intermedio e finale (negli appositi campi testuali).

Rapporto intermedio - Campi blu

Informazioni generali

- *Qual è il problema specifico?* inserire una descrizione più dettagliata dell'incidente avendo cura di indicare almeno le sue caratteristiche principali e le informazioni sul problema specifico.
- *Come è iniziato l'incidente?* inserire una descrizione su come l'incidente è iniziato includendo anche il background sulla rilevazione (come e chi si è accorto dell'incidente, chi ha coinvolto, ecc.).
- *Come si è evoluto?* Indicare come l'incidente si è evoluto dopo la rilevazione.
- *Quali sono le conseguenze?* inserire una descrizione dettagliata delle conseguenze dell'incidente, con particolare riferimento alle conseguenze per gli utenti dei servizi.
- *L'incidente è stato comunicato agli utenti del servizio di pagamento?* indicare se l'incidente è stato comunicato agli utenti del servizio di pagamento ed eventualmente fornire dei dettagli di tale comunicazione. Utilizzare il valore N.A. per gli incidenti che non hanno impatti sui servizi di pagamento.
- *L'incidente è correlato a precedenti incidenti?* Indicare se l'incidente è correlato a precedenti incidenti e in caso affermativo fornire gli identificativi di quest'ultimi.

- *Data/ora inizio incidente – se nota?* indicare, se nota, la data e ora in cui l'incidente è iniziato.
- *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 intermedio e finale.

Classificazione dell'incidente/Informazioni sull'incidente

- *Causa dell'incidente:*
    - *Azioni malevoli*: incidenti causati da azioni mirate intenzionalmente verso l'intermediario. Essi comprendono ad esempio gli attacchi *cyber*, azioni deliberate compite da personale interno, danneggiamenti causati da personale esterno, ecc.
    - *Malfunzionamento nel 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).
    - *Malfunzionamento del sistema*: la causa dell'incidente è associata con una progettazione, esecuzione, componenti, specifiche, integrazione o complessità non adeguata dei sistemi, reti, infrastrutture e banche dati che supportano le attività dell'intermediario.
    - *Errori umani*: incidenti causati o in qualche modo correlati principalmente ad errori umani non intenzionali.
    - *Eventi esterni*: la causa è associata a eventi generalmente al di fuori del controllo diretto dell'intermediario (es. calamità naturali, guasto del fornitore di servizi tecnici).
    - *In fase di analisi*: la causa non è ancora nota al momento dell'invio del rapporto.
    - *Altro*: la causa è diversa da quelle indicate, specificare dettagli nell'apposito campo testuale.
- *Transazioni interessate:* nel caso di servizi di pagamento, indicare il livello di impatto sulla base dei criteri e soglie per la segnalazione, il numero di transazioni interessate, la percentuale di tali transazioni in relazione al numero di transazioni di pagamento effettuate con i servizi di pagamento interessati dall'incidente e il valore totale delle transazioni. Nel caso di incidenti operativi indicare se l'incidente ha avuto una durata maggiore, minore od uguale ad un'ora. Per queste variabili, si devono fornire valori significativi, che possono essere dati effettivi o stime (si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" per maggiori dettagli).
- *Utenti interessati:* indicare il livello di impatto sulla base dei criteri e soglie per la segnalazione, il numero totale di utenti che sono stati interessati e la percentuale di utenti del/dei servizio/i interessato/i dall'incidente rispetto al numero totale di utenti del/dei servizio/i interessato/i. Per queste variabili, fornire valori che possono essere dati effettivi o stime (si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" per maggiori dettagli).

- *Violazione della sicurezza della rete o dei sistemi informativi*: indicare se eventuali azioni dannose hanno compromesso la disponibilità, l'autenticità, l'integrità o la riservatezza della rete o dei sistemi informativi (inclusi i dati) dell'intermediario.
- *Indisponibilità del servizio:* indicare se vi è stata indisponibilità del servizio e, in caso affermativo, riportare i dati relativi al periodo totale di indisponibilità (espressi in giorni, ore e minuti). Per queste variabili, gli intermediari 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:* gli intermediari devono indicare se la soglia è stata o probabilmente sarà raggiunta dall'incidente e i dati relativi (espressi in euro). Per questa variabile, gli intermediari 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:* gli intermediari devono considerare se, in conseguenza dell'impatto dell'incidente, il responsabile della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell'accaduto in via straordinaria rispetto alle procedure 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).
- *Sono state attivate procedure di gestione della crisi (interne o/o esterne)?* Indicare se è stata avviata o meno la gestione della crisi (interna e/o esterna). Se è stata avviata la gestione della crisi, fornire ulteriori dettagli.
- *Impatto sulla reputazione:* gli intermediari devono 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). Inoltre, nel caso di violazioni di obblighi legali e regolamentari specificare le norme/disposizioni violate.
- *Altri intermediari, operatori o infrastrutture rilevanti coinvolti o potenzialmente interessati (impatto sistemico):* gli intermediari 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 intermediari (si faccia riferimento alla sezione "Criteri e soglie per la segnalazione" per maggiori dettagli).

Impatto incidente e azioni di mitigazione

- *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.

- *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 quest'ultimo caso, il nome del/dei fornitori.
- *Altri service provider/terze parti affette o coinvolte*?*:* indicare se l'incidente ha interessato o coinvolto altri fornitori di servizi/terze parti, nel caso in cui queste informazioni siano disponibili. In caso affermativo, indicarne il nome e fornire ulteriori informazioni.
- *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.
- *Quali azioni/misure sono state adottate finora o sono previste per il ripristino a seguito dell'incidente?:* fornire informazioni dettagliate sulle azioni intraprese o pianificate per affrontare temporaneamente l'incidente.
- *Sono stati attivati il piano di continuità operativa e/o il piano di Disaster Recovery? In caso affermativo, quando? Con quali modalità?:* si veda la sezione "Criteri e soglie per la segnalazione" per maggiori dettagli.

Rapporto finale - Campi verdi

Informazioni generali

- *Informazioni aggiuntive*: fornire informazioni dettagliate relative all'incidente grave e note al momento dell'invio del rapporto finale. Si devono aggiungere informazioni più approfondite sull'incidente, aggiornando, eventualmente, quelle fornite nel rapporto intermedio, nonché un'accurata analisi delle cause.
- *Tutti i controlli originali sono ripristinati?*: Indicare se le misure di controllo eventualmente rimosse o attenuate per far fronte all'incidente sono state tutte ripristinate, in caso negativo indicare le misure ancora non ripristinate e la data in cui si prevede il loro ripristino. Se nessuna misura di controllo è stata rimossa/attenuata durante l'incidente selezionare la voce "*I controlli originali non sono stati mai cancellati o attenuati*".

Causa principale – follow-up e informazioni aggiuntive

- *Qual è stata la causa all'origine dell'incidente (se conosciuta)?* Indicare qual è la causa all'origine dell'incidente o, se questa non è ancora nota, quella più probabile:
    - *Azioni malevoli*: azioni esterne o interne mirate intenzionalmente all'intermediario. Selezionare una o più delle seguenti voci:
        - *Codice malevolo*: come ad es. *virus, worm, spyware,trojan.*
        - *Raccolta di informazioni*: come ad es. *scanning, sniffing,* e tecniche di *social engineering*.
        - *DoS/DDoS*: attacchi alla negazione del servizio
        - *Intrusioni*: ad es. compromissione di account privilegiati, compromissione di account non privilegiati, compromissione di applicazioni, bot.
        - *Atto interno volontario:* ad es. sabotaggio, furto.
        - *Danno fisico volontario esterno:* come ad es. sabotaggio, attacco fisico dei locali/data center.
        - *Sicurezza contenuto delle informazioni:* come ad es. accesso e/o modifica non autorizzata ai dati/informazioni.
        - *Azioni fraudolente:* come ad es. utilizzo non autorizzato di risorse, copyright, *masquerade*, *phishing*.
        - *Altro (Specificare):* Altro causa malevola (specificare nell'apposito campo testuale
    - *Malfunzionamento nel 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). Selezionare una o più delle seguenti voci:
        - *Monitoraggio e controllo carenti*: carenze nei processi di monitoraggio e controllo ad esempio in relazione alle operazioni in esecuzione, alla scadenza di certificati, alla scadenza di licenze, alle scadenze delle patch, alla definizione dei valori massimi di contatori, ai livelli di riempimento del database, alla gestione dei diritti utente, al principio del doppio controllo.
        - *Problemi di comunicazione*: problemi di comunicazione ad es. tra operatori di mercato o all'interno dell'organizzazione;
        - *Operazioni improprie*: riscontrate operazioni non valide come ad es. mancato scambio di certificati, cache piena, ecc.
        - *Gestione del cambiamento inadeguata*: Inadeguatezza del processo di *change management* (gestione del cambiamento) evidenziata ad es. da errori di configurazione non identificati, problemi con il roll-out (inclusi aggiornamenti), problemi di manutenzione, errori imprevisti.

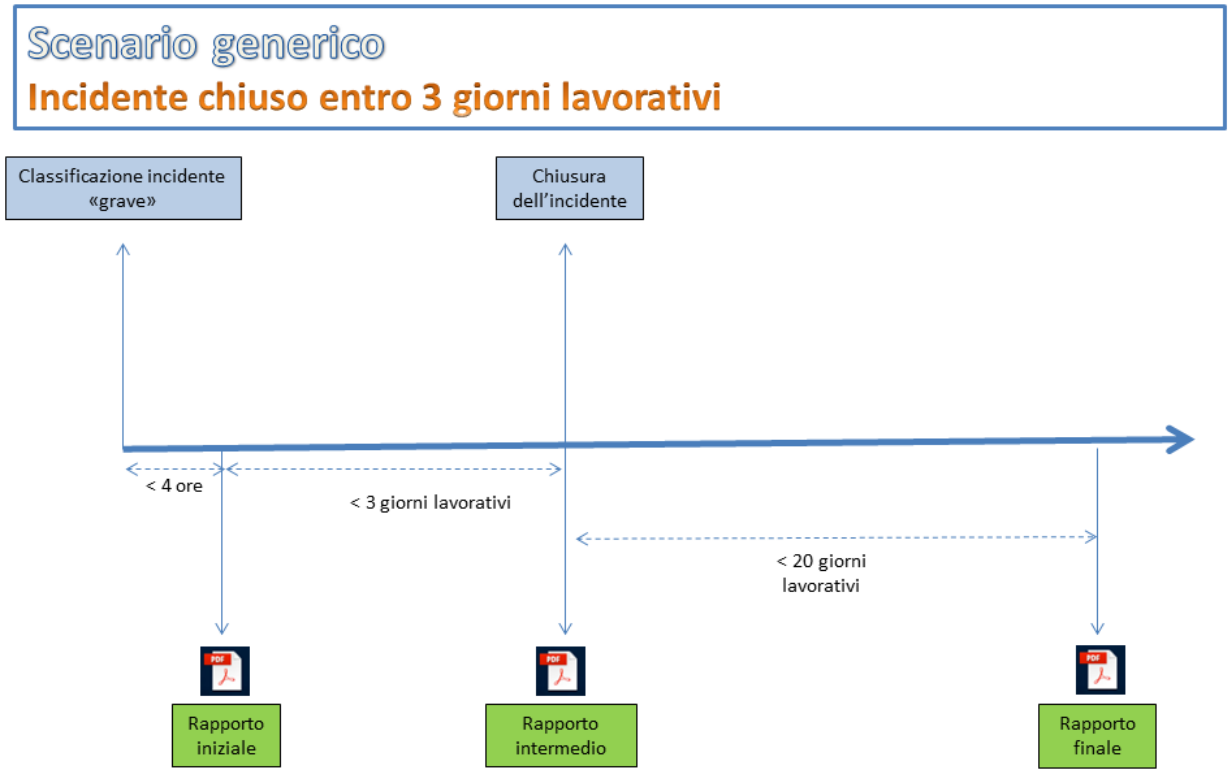
- *Inadeguatezza delle procedure interne e della documentazione*: procedure interne e/o documentazione non adeguate (es. mancanza di trasparenza in merito a funzionalità, processi e insorgenza di malfunzionamenti, assenza di documentazione, ecc.).
- *Problemi di ripristino*: Problemi con il processo di *recovery*, quali ad es. gestione delle emergenze, ridondanza inadeguata, ecc.
- *Altro (specificare):* Altro causa malfunzionamento processo (specificare nell'apposito campo testuale.

- *Malfunzionamento del sistema*: la causa dell'incidente è associata con una progettazione, esecuzione, componenti, specifiche, integrazione o complessità non adeguata dei sistemi, reti, infrastrutture e banche dati che supportano le attività dell'intermediario. Selezionare una o più delle seguenti voci:
  - *Malfunzionamento hardware*: guasto dell'apparecchiatura tecnologica fisica che esegue i processi e/o archivia i dati necessari all'intermediario per svolgere la propria attività.
  - *Malfunzionamento rete*: guasto delle reti di telecomunicazione, pubbliche o private, che consentono lo scambio di dati e informazioni (ad es. tramite Internet).
  - *Malfunzionamento database*: problemi con la struttura dei dati che memorizza le informazioni/i dati necessari all'intermediario per svolgere la propria attività.
  - *Malfunzionamenti software/applicativi*: guasti di programmi, sistemi operativi, ecc. che supportano l'erogazione dei servizi da parte dell'intermediario (es. malfunzionamenti, funzioni sconosciute).
  - *Danno fisico*: ad es. danni involontari causati da condizioni inadeguate, lavori di costruzione.
  - *Altro (specificare):* Altro causa malfunzionamento sistemi (specificare nell'apposito campo testuale.
- *Errori umani*: incidenti causati o in qualche modo legati principalmente ad errori umani non intenzionali. Selezionare una o più delle seguenti voci:
  - *Non intenzionale*: ad es. disattenzioni, errori, omissioni, mancanza di esperienza e conoscenza.
  - *Mancata azione*: ad es. per mancanza di competenze, conoscenze, esperienze, consapevolezza.
  - *Risorse insufficienti*: ad es. mancanza di risorse umane, scarsa disponibilità di personale.
  - *Altro (specificare):* Altro causa di errore umano (specificare nell'apposito campo testuale.

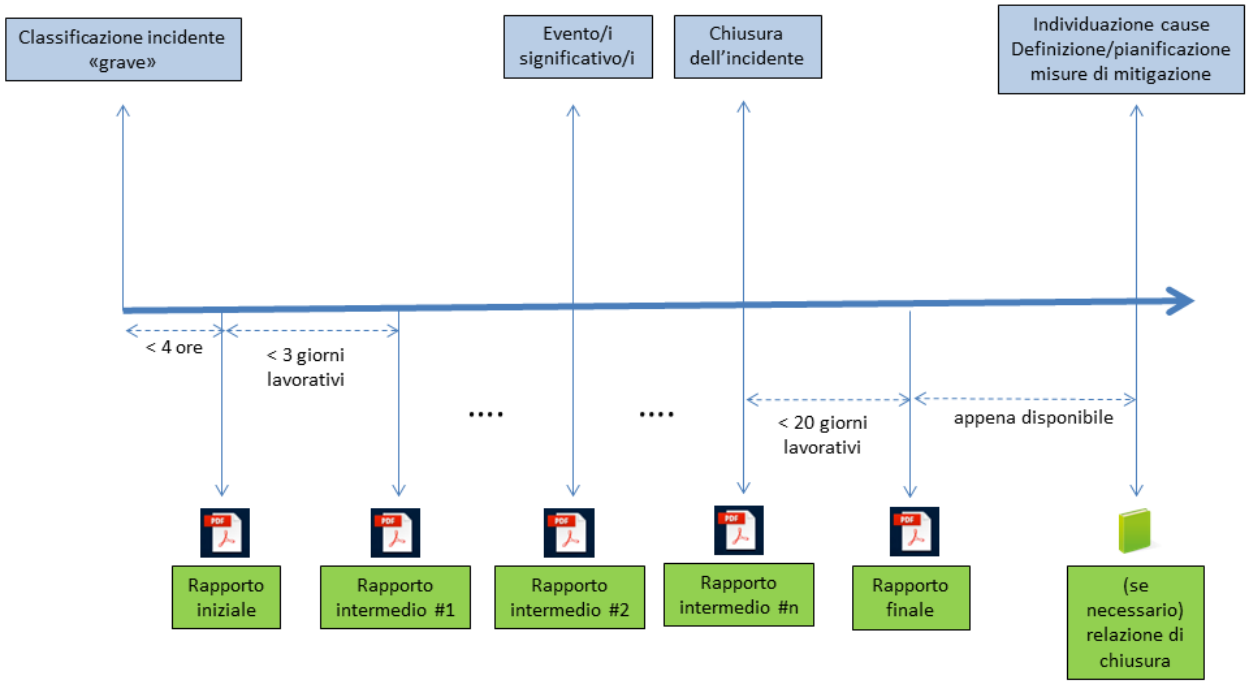
- *Eventi esterni*: la causa è associata a eventi generalmente al di fuori del controllo diretto dell'intermediario (es. calamità naturali, guasto del fornitore di servizi tecnici). Selezionare una o più delle seguenti voci:
  - *Causa di forza maggiore*: ad es. mancanza di corrente, incendi, cause naturali come terremoti, inondazioni, forti precipitazioni, vento forte.
  - *Inadempienza di un fornitore/prestatore di servizi tecnici*: ad es. interruzione di corrente, interruzione di Internet, problemi legali, problemi aziendali, dipendenze dal servizio.
  - *Altro (specificare):* Altro causa esterna (specificare nell'apposito campo testuale.
- *Altra cause (specificare)*: la causa è diversa da quelle indicate, specificare dettagli nell'apposito campo testuale.

- *Altre rilevanti informazioni sulla causa all'origine dell'incidente:* fornire eventuali ulteriori dettagli sulla causa all'origine dell'incidente, comprese le conclusioni preliminari tratte dalla relativa analisi.
- *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 condiviso con altri intermediari a scopo informativo? E con il CERTFIN?*: indicare se le informazioni sull'incidente sono state condivise con altri intermediari e/o all'interno del CertFIN. In caso affermativo fornire i dettagli.
- *Azioni legali intraprese nei confronti dell'intermediario?* indicare se l'intermediario è a conoscenza di azioni legale intraprese nei propri confronti a seguito dell'incidente.
- *Valutazione dell'efficacia delle azioni intraprese*: indicare il risultato di un'autovalutazione dell'efficacia delle azioni intraprese durante la durata dell'incidente, comprese le lezioni apprese dall'incidente, motivando, se del caso, il risultato nell'apposito campo testuale.

ALLEGATO 1 – Illustrazione di scenari possibili di segnalazione

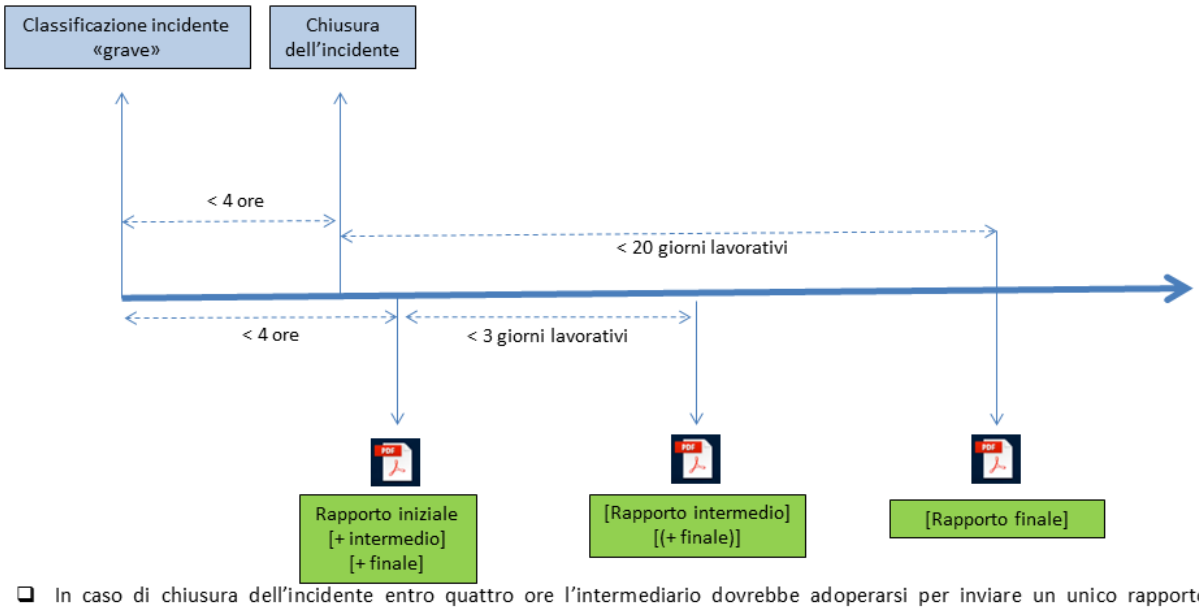


Scenario #1
Incidente chiuso dopo 3 giorni lavorativi + cause individuate dopo il rapporto finale



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

Scenario #2
Incidente chiuso entro 4 ore



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