

I campi obbligatori per ciascun tipo di rapporto sono indicati con i seguenti colori:

Rapporto iniziale	entro 4 ore dalla rilevazione dell'incidente
Rapporto intermedio	entro tre giorni lavorativi dopo il precedente rapporto
Ultimo rapporto intermedio	dopo la chiusura dell'incidente
Rapporto finale	entro 2 settimane dalla chiusura dell'incidente

Data e ora del rapporto

Numero di identificazione dell'incidente (solo per rapporti intermedi o finali)

Quando è previsto il prossimo aggiornamento?

Prossimo aggiornamento - motivazione

Incidente riclassificato come non grave

Riclassificato come non grave - motivazione

Segnalazione di grave incidente operativo o di sicurezza informatica - Banche LSI

INFORMAZIONI GENERALI				
Nome dell'istituto segnalante	<div>Gruppo bancario?</div> <div>Email</div> <div>Telefono</div> <div>Se altro, specificare:</div> <div>Se Sì, indicare data e ora</div> <div>Data/ora in cui l'incidente è stato chiuso o in cui si prevede di chiuderlo</div>			
Codice ABI segnalante (5 cifre)				
Numero di iscrizione all'Albo del segnalante				
Paese/paesi interessato/i dall'incidente				
Referente principale da contattare				
Referente secondario da contattare				
Data e ora di rilevazione dell'incidente				
L'incidente è stato rilevato da				
Sono noti data e ora di inizio dell'incidente?			Si	No
Status dell'incidente				
L'incidente è chiuso?	Si	No		
DESCRIZIONE DELL'INCIDENTE				
Categoria dell'incidente				
L'incidente interessa servizi di pagamento?	Si	No		
<div>Rapporto iniziale</div> <div>Fornire una breve descrizione generale dell'incidente</div> <div>Descrivere brevemente gli aspetti più rilevanti dell'incidente (eventualmente indicando possibili cause, impatti immediati, ecc.)</div>				
<div>Rapporto intermedio</div> <div>Fornire una descrizione più DETTAGLIATA dell'incidente, riportando informazioni relative a quanto segue:</div> <div>- Qual è il problema specifico?</div> <div>- Come è accaduto? Come si è sviluppato?</div> <div>- È collegato a un incidente precedente?</div> <div>- Conseguenze (in particolare per gli utenti di servizi di pagamento)</div> <div>- Contesto della rilevazione dell'incidente</div> <div>- Aree interessate</div> <div>- Azioni intraprese finora</div> <div>- Intermediari/operatori/terze parti interessati o coinvolti</div> <div>- È stata avviata la modalità di crisi aziendale? (interna e/o esterna) (gestione della crisi da parte della banca centrale)</div> <div>- Classificazione interna dell'incidente</div>				
<div>Rapporto finale</div> <div>Aggiornare le informazioni del rapporto intermedio (sintesi):</div> <div>- ulteriori azioni/misure intraprese per il ripristino a seguito dell'incidente</div> <div>- interventi correttivi finali attuati</div> <div>- analisi delle cause all'origine dell'incidente</div> <div>- lezioni apprese</div> <div>- ulteriori azioni</div> <div>- altre informazioni pertinenti</div>				

INFORMAZIONI SULL'INCIDENTE					
L'incidente vi ha interessati direttamente o attraverso un fornitore di servizi?	Direttamente	Attraverso un fornitore	Se tramite un fornitore di servizi, indicare il nome del fornitore di servizi		
Tipo di incidente - cyber <i>(è possibile la selezione multipla)</i>	<u>Malware</u>	<u>Social engineering</u>	<u>Personale interno/Fornitore esterno</u>	<u>Accesso non autorizzato</u>	<u>Denial of service</u>
	Ransomware	Phishing / *ishing	Diffusione/alterazione accidentale di dati	Attacco "brute force"	
	Trojan horse	Spear phishing	Abuso diritti di accesso - personale interno	Malicious script injection - OS commanding	
	Virus/worm	Pretexting	Abuso diritti di accesso - fornitore esterno	Altre vulnerabilità sfruttate	<u>Altro</u>
	Mobile malware	Altri "social engineering"			
	Se altro, specificare:				
	Incidente classificato come "Advanced Persistent Threat"?				
Tipo di incidente - incidente operativo <i>(è possibile la selezione multipla)</i>	Eventi accidentali (ad es.,errore umano)				
	*con l'eccezione di "Diffusione/alterazione di dati accidentale",classificata come incidente cyber				
	Malfunzionamento del processo				
	Problema software				
	Problema hardware o infrastrutturale				
	Sabotaggio				
	Evento naturale				
	Altro				
	Se altro, specificare::				

CLASSIFICAZIONE E IMPATTO DELL'INCIDENTE							
Impatto generale <i>(è possibile la selezione multipla)</i>	Integrità		Disponibilità		Riservatezza	Autenticità	Continuità
Transazioni interessate <i>(solo nel caso siano interessati dall'incidente servizi di pagamento)</i>							
	Numero delle transazioni interessate						
	In % del numero normale di transazioni						
	Valore transazioni interessate in EUR						
	Osservazioni						
Utenti interessati							
	Numero degli utenti interessati						
	In % degli utenti del servizio						
Periodo di indisponibilità della componente critica del sistema informativo							
	Durata periodo di indisponibilità		GG:HH:MM				
Impatto economico							
	Costi diretti in EUR						
	Costi indiretti in EUR						
Alto livello di escalation interna							
	Descrivere il livello di escalation interna dell'incidente e indicare se ha determinato o probabilmente determinerà l'attivazione della modalità di crisi (o equivalente); in caso affermativo, fornire una descrizione						
Altri intermediari, operatori o infrastrutture rilevanti coinvolti o potenzialmente interessati (impatto sistemico)							
	Descrivere come l'incidente coinvolge o potrebbe interessare altri intermediari, operatori e/o infrastrutture						
Possibili violazioni di obblighi legali o regolamentari.							
	Se Sì, descrivere come l'incidente potrebbe comportare violazioni di obblighi legali o regolamentari						
Impatto sulla reputazione							
	Descrivere come l'incidente potrebbe influenzare la reputazione dell'intermediario (ad esempio, copertura mediatica, possibile violazione in termini giuridici o regolamentari, ecc.)						
Altri impatti (se presenti, specificare)							

DETTAGLI SULL'IMPATTO DELL'INCIDENTE					
Edificio/i interessato/i (indirizzo), se applicabile					
Sistemi e componenti interessati <i>(è possibile la selezione multipla)</i>	Applicativi/software	Hardware	Database	Network/infrastrutture	Altro
	Se altro, specificare:				
Funzioni aziendali colpite <i>(è possibile la selezione multipla)</i>	Corporate finance Payment & Settlement	Trading & Sales Agency Services	Retail Banking Asset Management	Commercial Banking Retail Brokerage	Altro
	Se altro, specificare:				
Canali commerciali interessati	Succursali E-banking	Telephone banking Mobile banking	Punto vendita ATM	Altro	
	Se altro, specificare:				
Servizi di pagamento interessati <i>(solo nel caso di incidente che interessi servizi di pagamento, è possibile la selezione multipla)</i>	Deposito contanti su conto di pagamento Prelievo contanti da conto di pagamento Operaz. necessarie per gestire conto di pag. Acquiring di strumenti di pagamento	Bonifici Addebiti diretti Pagamenti tramite carta Emissione di strumenti di pagamento	Rimessa di denaro Servizi di disposizione ordini di pagamento Servizi di informazione sui conti Altro		
	Se altro, specificare:				
Aree funzionali dei servizi di pagamento interessate <i>(solo nel caso di incidente che interessi servizi di pagamento, è possibile la selezione multipla)</i>	Autenticazione/autorizzazione Comunicazione	Compensazione Regolamento diretto	Regolamento indiretto Altro		
	Se altro, specificare:				
Personale interessato					
	Descrivere come l'incidente potrebbe interessare il personale del fornitore/intermediario (ad esempio, personale non in grado di raggiungere l'ufficio per assistere i clienti, ecc.)				

ANALISI, MITIGAZIONE E RISOLUZIONE DELL'INCIDENTE					
Quali azioni/misure sono state adottate finora o sono previste per il ripristino a seguito dell'incidente?					
Sono stati attivati il piano di continuità operativa e/o il piano di Disaster Recovery? In caso affermativo, quando? Con quali modalità?	Si	No	Data e ora:		Descrivere
L'intermediario ha annullato o attenuato alcune misure di controllo a causa dell'incidente?	Si	No	Se Si, spiegare		
Qualora l'intermediario abbia eliminato/attenuato misure di controllo, tali misure sono state ripristinate?	Si	No	Se Si, spiegare		
Qual è la causa all'origine dell'incidente (se già nota)? (è possibile allegare un file con informazioni dettagliate)					
Principali azioni correttive/misure adottate o pianificate per evitare il ripetersi dell'incidente in futuro, se già note					
L'incidente è stato riportato al CERT/CSIRT nazionale?	Si	No			
L'incidente è stato condiviso con altri intermedari a scopo informativo? E con il CERTFIN?	Si	No	Se Si, spiegare		
È stata intrapresa un'azione legale nei confronti dell'intermediario?	Si	No	Se Si, spiegare		

## ELENCO DEGLI ENTI INTERESSATI DALL'INCIDENTE

[illegible]