REGOLAMENTO DI ESECUZIONE (UE) 2025/302 DELLA COMMISSIONE

del 23 ottobre 2024

che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ([1]), in particolare l'articolo 20, quarto comma,

considerando quanto segue:

(1) Al fine di garantire che le entità finanziarie segnalino gli incidenti gravi alle rispettive autorità competenti in modo coerente e far sì che trasmettano a tali autorità dati di buona qualità, è opportuno specificare quali campi di dati debbano essere compilati dalle entità finanziarie nelle varie fasi della segnalazione di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554. È importante che tali informazioni siano presentate in modo da fornire un'unica panoramica dell'incidente. A tal fine è pertanto necessario definire un modello unico per la segnalazione.

(2) Le entità finanziarie dovrebbero compilare i campi di dati del modello di segnalazione che corrispondono agli obblighi di informazione della rispettiva notifica o relazione. Tuttavia le entità finanziarie che dispongono già di informazioni che devono essere fornite in una fase successiva della segnalazione, ossia nella relazione intermedia o finale, dovrebbero essere autorizzate ad anticipare la trasmissione dei dati.

(3) Poiché gli incidenti multipli o ricorrenti possono costituire un incidente grave ai sensi dell'articolo 8 del regolamento delegato (UE) 2024/1772 della Commissione ([2]), l'impostazione del modello di segnalazione e dei campi di dati dovrebbe consentire alle entità finanziarie di segnalare tali incidenti ricorrenti.

(4) Per garantire la presentazione di informazioni accurate e aggiornate, il modello di segnalazione dovrebbe consentire alle entità finanziarie, all'atto della trasmissione della relazione intermedia e finale, di aggiornare le informazioni presentate in precedenza e, se necessario, di riclassificare gli incidenti gravi come non gravi.

(5) L'identificazione giuridica delle entità dovrebbe essere allineata agli identificatori specificati nelle norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.

(6) Qualora le entità finanziarie esternalizzino a terzi gli obblighi di segnalazione di incidenti gravi connessi alle TIC, le autorità competenti dovrebbero essere a conoscenza dell'identità del terzo che effettua la segnalazione per conto dell'entità finanziaria prima della trasmissione della prima notifica o relazione, al fine di verificare la legittimità del terzo che effettua la segnalazione.

([1]) GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Regolamento delegato (UE) 2024/1772 della Commissione, del 13 marzo 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti (GU L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) Per individuare agevolmente l'impatto di un incidente verificatosi presso un fornitore terzo o da esso causato e che interessa più entità finanziarie all'interno di un unico Stato membro, e per ridurre lo sforzo di segnalazione per le entità finanziarie, il modello di segnalazione dovrebbe consentire la trasmissione di una relazione aggregata contenente informazioni aggregate in merito all'impatto dell'incidente su tutte le entità finanziarie interessate che hanno classificato l'incidente come grave.

(8) Il modello di segnalazione dovrebbe essere impostato in modo tecnologicamente neutro al fine di consentirne l'implementazione in varie soluzioni di segnalazione degli incidenti già esistenti o che possono essere sviluppate ai fini dell'attuazione degli obblighi di cui al regolamento (UE) 2022/2554.

(9) L'impostazione del modello di segnalazione e dei campi di dati dovrebbe agevolare la segnalazione degli incidenti gravi connessi alle TIC da parte dei terzi ai quali le entità finanziarie hanno esternalizzato l'obbligo di segnalazione a norma dell'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554.

(10) Il presente regolamento si basa sui progetti di norme tecniche di attuazione che le autorità europee di vigilanza hanno presentato alla Commissione.

(11) Le autorità europee di vigilanza hanno condotto consultazioni pubbliche aperte sui progetti di norme tecniche di attuazione sui quali è basato il presente regolamento, hanno analizzato i potenziali costi e benefici collegati e hanno chiesto la consulenza del gruppo delle parti interessate nel settore bancario istituito in conformità dell'articolo 37 rispettivamente dei regolamenti (UE) n. 1093/2010 ([3]), (UE) n. 1094/2010 ([4]) e (UE) n. 1095/2010 ([5]), del Parlamento europeo e del Consiglio.

(12) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]), il Garante europeo della protezione dei dati è stato consultato e ha formulato un parere positivo il 22 luglio 2024. Qualsiasi trattamento di dati personali che rientra nell'ambito di applicazione del presente regolamento dovrebbe essere effettuato conformemente ai principi applicabili in materia di protezione dei dati e alle disposizioni di cui al regolamento (UE) 2018/1725,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Modello per la segnalazione degli incidenti gravi connessi alle TIC

1. Le entità finanziarie utilizzano il modello di cui all'allegato I per trasmettere la notifica iniziale, la relazione intermedia e la relazione finale di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554 come segue:

a) le entità finanziarie che presentano una notifica iniziale compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 2 del regolamento delegato (UE) 2025/301 della Commissione ([7]) e possono, qualora dispongano già di tali informazioni, completare i campi di dati la cui compilazione non è richiesta per una notifica iniziale ma è richiesta per una relazione intermedia o finale;

([3]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Regolamento delegato (UE) 2025/301 della Commissione, del 23 ottobre 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative (GU L, 2025/301, 20.2.2025 ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) le entità finanziarie che presentano una relazione intermedia compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 3 del regolamento delegato (UE) 2025/301 e possono, qualora dispongano già di tali informazioni, completare i campi di dati la cui compilazione non è richiesta per la relazione intermedia ma è richiesta per la relazione finale.

c) le entità finanziarie che presentano una relazione finale compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 4 del regolamento delegato (UE) 2025/301

2. Le entità finanziarie garantiscono che le informazioni contenute nella notifica iniziale, nella relazione intermedia e nella relazione finale siano complete e accurate.

3. Le entità finanziarie forniscono stime dei valori sulla base di altri dati e informazioni disponibili, nella misura del possibile, qualora non siano disponibili dati accurati al momento della trasmissione della notifica iniziale o della relazione intermedia.

4. All'atto della trasmissione di una relazione intermedia o finale, le entità finanziarie utilizzano il modello di cui all'allegato I per fornire tutte le informazioni richieste e aggiornare, se del caso, le informazioni precedentemente fornite nella notifica iniziale o nella relazione intermedia.

5. All'atto della compilazione del modello di cui all'allegato I le entità finanziarie seguono il glossario dei dati e le istruzioni di cui all'allegato II.

Articolo 2

Trasmissione congiunta della notifica iniziale, della relazione intermedia e della relazione finale

Le entità finanziarie possono combinare la presentazione della notifica iniziale, della relazione intermedia e della relazione finale per fornire due o tutte le informazioni contemporaneamente, qualora siano riprese le attività regolari o sia stata completata l'analisi delle cause profonde e purché siano rispettati i termini di cui all'articolo 5 del regolamento delegato (UE) 2025/301

Articolo 3

Incidenti ricorrenti connessi alle TIC

Le entità finanziarie che forniscono informazioni su incidenti ricorrenti connessi alle TIC non gravi che soddisfano cumulativamente le condizioni per la sussistenza di un incidente grave connesso alle TIC di cui all'articolo 8, paragrafo 2, del regolamento delegato (UE) 2024/1772 trasmettono tali informazioni in forma aggregata.

Articolo 4

Uso di canali elettronici sicuri

1. Le entità finanziarie utilizzano canali elettronici sicuri messi a disposizione dalla rispettiva autorità competente per la trasmissione della notifica iniziale e delle relazioni intermedia e finale.

2. Le entità finanziarie che non sono in grado di utilizzare i canali elettronici sicuri messi a disposizione dalla rispettiva autorità competente informano la propria autorità competente in merito a un incidente grave connesso alle TIC mediante altri mezzi sicuri, d'intesa con l'autorità competente. Se richiesto dall'autorità competente, le entità finanziarie trasmettono nuovamente la notifica iniziale oppure la relazione intermedia o finale, attraverso il canale elettronico sicuro messo a disposizione dalla rispettiva autorità competente appena sono in grado di farlo.

Articolo 5

Riclassificazione degli incidenti gravi connessi alle TIC

Se, dopo un'ulteriore valutazione, l'entità finanziaria conclude che l'incidente connesso alle TIC precedentemente segnalato come grave non soddisfaceva in alcun momento i criteri e le soglie di classificazione di cui all'articolo 8 del regolamento delegato (UE) 2024/1772, l'entità finanziaria notifica all'autorità competente di aver riclassificato l'incidente connesso alle TIC da grave a non grave fornendo le informazioni relative a tale riclassificazione nel modello di cui all'allegato II del presente regolamento nei campi «tipo di segnalazione» e «altre informazioni».

Articolo 6

Notifica dell'esternalizzazione degli obblighi di segnalazione

1. Le entità finanziarie che hanno esternalizzato l'obbligo di segnalazione degli incidenti gravi connessi alle TIC a norma dell'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554 informano l'autorità competente di tale accordo di esternalizzazione non appena quest'ultimo è stato concluso e al più tardi prima della prima notifica o relazione.

2. Le entità finanziarie forniscono all'autorità competente il nome, le informazioni di contatto e il codice identificativo del terzo che trasmetterà per loro conto le notifiche o le relazioni in merito agli incidenti gravi connessi alle TIC.

3. Le entità finanziarie informano la rispettiva autorità competente non appena cessano di esternalizzare i propri obblighi di segnalazione di cui all'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554.

Articolo 7

Segnalazione aggregata

1. Un fornitore terzo di servizi cui sono stati esternalizzati obblighi di segnalazione conformemente all'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554 può utilizzare il modello di cui all'allegato I del presente regolamento per fornire informazioni aggregate in merito a un incidente grave connesso alle TIC che ha un impatto su più entità finanziarie in un'unica notifica o relazione e trasmettere tale notifica o relazione all'autorità competente per conto di tutte le entità finanziarie interessate, purché siano soddisfatte tutte le condizioni seguenti:

a) l'incidente grave connesso alle TIC da segnalare ha origine presso un fornitore terzo di servizi TIC o è causato da quest'ultimo;

b) il fornitore terzo di servizi presta il servizio TIC pertinente a più di un'entità finanziaria o a un gruppo;

c) l'incidente connesso alle TIC è classificato come grave da ciascuna entità finanziaria interessata nella notifica o relazione aggregata;

d) l'incidente grave connesso alle TIC interessa entità finanziarie all'interno di un unico Stato membro e la relazione aggregata si riferisce a entità finanziarie sottoposte alla vigilanza della medesima autorità competente;

e) le autorità competenti hanno esplicitamente consentito a questo tipo di entità finanziarie di aggregare le loro segnalazioni.

2. Il paragrafo 1 non si applica agli enti creditizi considerati significativi di cui all'articolo 2, punto 16), del regolamento (UE) n. 468/2014 della Banca centrale europea ([8]), ai gestori delle sedi di negoziazione e alle controparti centrali, che utilizzano il modello di cui all'allegato I solo per trasmettere notifiche o relazioni individuali in merito a incidenti gravi connessi alle TIC alla rispettiva autorità competente.

3. Qualora le autorità competenti richiedano informazioni sull'impatto individuale dell'incidente grave connesso alle TIC su un'unica entità finanziaria, su richiesta dell'autorità competente l'entità finanziaria trasmette una notifica o una relazione individuale in merito all'incidente grave connesso alle TIC.

([8]) Regolamento (UE) n. 468/2014 della Banca centrale europea, del 16 aprile 2014, che istituisce il quadro di cooperazione nell'ambito del Meccanismo di vigilanza unico tra la Banca centrale europea e le autorità nazionali competenti e con le autorità nazionali designate (Regolamento quadro sull'MVU) (BCE/2014/17) (GU L 141 del 14.5.2014, pag. 1 , ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Articolo 8

Notifica delle minacce informatiche significative

1. Le entità finanziarie che notificano minacce informatiche significative alle autorità competenti a norma dell'articolo 19, paragrafo 2, del regolamento (UE) 2022/2554 utilizzano il modello di cui all'allegato III del presente regolamento e seguono il glossario dei dati e le istruzioni di cui all'allegato IV del presente regolamento.

2. Le entità finanziarie garantiscono che le informazioni contenute nella notifica delle minacce informatiche significative siano complete e accurate.

Articolo 9

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 23 ottobre 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

MODELLI PER LA SEGNALAZIONE DI INCIDENTI GRAVI

Numero del campo	Campo di dati	
Informazioni generali sull'entità finanziaria		
1.1	Tipo di segnalazione	
1.2	Denominazione dell'entità che trasmette la segnalazione	
1.3	Codice identificativo dell'entità che trasmette la segnalazione	
1.4	Tipo di entità finanziaria interessata	
1.5	Denominazione dell'entità finanziaria interessata	
1.6	Codice LEI dell'entità finanziaria interessata	
1.7	Nome del referente principale	
1.8	E-mail: del referente principale	
1.9	Telefono del referente principale	
1.10	Nome del secondo referente	
1.11	E-mail: del secondo referente	
1.12	Telefono del secondo referente	
1.13	Denominazione dell'impresa madre capogruppo	
1.14	Codice LEI dell'impresa madre capogruppo	
1.15	Valuta della segnalazione	
Contenuto della notifica iniziale		
2.1	Codice di riferimento dell'incidente assegnato dall'entità finanziaria	
2.2	Data e ora di individuazione dell'incidente grave connesso alle TIC	
2.3	Data e ora della classificazione dell'incidente connesso alle TIC come grave	
2.4	Descrizione dell'incidente grave connesso alle TIC	
2.5	Criteri di classificazione che hanno determinato la segnalazione dell'incidente	
2.6	Soglie di rilevanza per il criterio di classificazione «Estensione geografica»	
2.7	Constatazione dell'incidente grave connesso alle TIC	

Numero del campo	Campo di dati	
2.8	Indicazione dell'origine dell'incidente grave connesso alle TIC presso un fornitore terzo o presso un'altra entità finanziaria	
2.9	Attivazione del piano di continuità operativa, se attivato	
2.10	Altre informazioni pertinenti	
Contenuto della relazione intermedia		
3.1	Codice di riferimento dell'incidente fornito dall'autorità competente	
3.2	Data e ora in cui si è verificato l'incidente grave connesso alle TIC	
3.3	Data e ora di ripristino dei servizi, delle attività o delle operazioni	
3.4	Numero di clienti interessati	
3.5	Percentuale di clienti interessati	
3.6	Numero di controparti finanziarie interessate	
3.7	Percentuale di controparti finanziarie interessate	
3.8	Impatto su clienti o controparti finanziarie rilevanti	
3.9	Numero di transazioni interessate	
3.10	Percentuale di transazioni interessate	
3.11	Valore delle transazioni interessate	
3.12	Informazioni indicanti se i numeri sono effettivi o stimati o se non vi è stato alcun impatto	
3.13	Impatto reputazionale	
3.14	Informazioni contestuali sull'impatto reputazionale	
3.15	Durata dell'incidente grave connesso alle TIC	
3.16	Periodo di inattività del servizio	
3.17	Informazioni indicanti se i numeri relativi alla durata e al periodo di inattività del servizio sono effettivi o stimati.	
3.18	Tipi di impatto negli Stati membri	
3.19	Descrizione dell'impatto dell'incidente grave connesso alle TIC in altri Stati membri	
3.20	Soglie di rilevanza per il criterio di classificazione «Perdite di dati»	
3.21	Descrizione delle perdite di dati	

Numero del campo	Campo di dati	
3.22	Criterio di classificazione «Servizi critici colpiti»	
3.23	Tipo di incidente grave connesso alle TIC	
3.24	Altri tipi di incidenti	
3.25	Minacce e tecniche utilizzate dall'autore della minaccia	
3.26	Altri tipi di tecniche	
3.27	Informazioni sulle aree funzionali interessate e sui processi commerciali interessati	
3.28	Componenti infrastrutturali interessate che sostengono i processi commerciali	
3.29	Informazioni sulle componenti infrastrutturali interessate che sostengono i processi commerciali	
3.30	Impatto sugli interessi finanziari dei clienti	
3.31	Segnalazione ad altre autorità	
3.32	Indicazione delle autorità di «altro» tipo	
3.33	Azioni/misure temporanee adottate o previste per effettuare il ripristino a seguito dell'incidente	
3.34	Descrizione di eventuali azioni e misure temporanee adottate o previste per effettuare il ripristino a seguito dell'incidente	
3.35	Indicatori di compromissione	
Contenuto della relazione finale		
4.1	Classificazione di alto livello delle cause di fondo dell'incidente	
4.2	Classificazione dettagliata delle cause di fondo dell'incidente	
4.3	Ulteriore classificazione delle cause di fondo dell'incidente	
4.4	Altri tipi di cause di fondo	
4.5	Informazioni sulle cause di fondo dell'incidente	
4.6	Sintesi della risoluzione dell'incidente	
4.7	Data e ora in cui è stata affrontata la causa di fondo dell'incidente	
4.8	Data e ora in cui l'incidente è stato risolto	
4.9	Informazioni indicanti se la data di risoluzione definitiva dell'incidente differisce dalla data di attuazione inizialmente prevista	
4.10	Valutazione del rischio per le funzioni essenziali ai fini della risoluzione	
4.11	Informazioni pertinenti per le autorità di risoluzione	

Numero del campo	Campo di dati	
4.12	Soglia di rilevanza per il criterio di classificazione «Impatto economico»	
4.13	Importo dei costi diretti e indiretti e delle perdite lordi	
4.14	Importo dei recuperi finanziari	
4.15	Informazioni indicanti se gli incidenti non gravi sono stati ricorrenti	
4.16	Data e ora in cui si sono verificati incidenti ricorrenti	

ALLEGATO II

GLOSSARIO DEI DATI E ISTRUZIONI PER LA SEGNALAZIONE DEGLI INCIDENTI GRAVI

Campo di dati		Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
Informazioni generali sull'entità finanziaria						
1.1.	Tipo di segnalazione	Indicare il tipo di notifica o di relazione in merito all'incidente trasmessa all'autorità competente.	Sì	Sì	Sì	Selezionare: — notifica iniziale; — relazione intermedia; — relazione finale; — incidente grave riclassificato come non grave.
1.2.	Denominazione dell'entità che trasmette la segnalazione	Denominazione giuridica completa dell'entità che trasmette la segnalazione.	Sì	Sì	Sì	Alfanumerico
1.3.	Codice identificativo dell'entità che trasmette la segnalazione	Codice identificativo dell'entità che trasmette la segnalazione. Se la notifica/relazione è trasmessa da entità finanziarie, il codice identificativo è un identificativo della persona giuridica (*Legal Entity Identifier*, LEI), che è un codice unico composto da 20 caratteri alfanumerici, basato sulla norma ISO 17442-1:2020. Un fornitore terzo che trasmette una segnalazione per un'entità finanziaria può utilizzare un codice identificativo come specificato nelle norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.	Sì	Sì	Sì	Alfanumerico
1.4.	Tipo di entità finanziaria interessata	Tipo di entità di cui all'articolo 2, paragrafo 1, lettere da a) a t), del regolamento (UE) 2022/2554 per la quale è trasmessa la segnalazione. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, selezionare i diversi tipi di entità finanziarie indicate nella segnalazione aggregata.	Sì	Sì	Sì	Selezionare (scelta multipla): — ente creditizio; — istituto di pagamento; — istituto di pagamento esentato; — prestatore di servizi di informazione sui conti; — istituto di moneta elettronica; — istituto di moneta elettronica esentato; — impresa di investimento; — fornitore di servizi per le cripto-attività; — emittente di token collegati ad attività; — depositario centrale di titoli; — controparte centrale; — sede di negoziazione; — repertorio di dati sulle negoziazioni;

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
					— gestore di fondi di investimento alternativi; — società di gestione; — fornitore di servizi di comunicazione dati; — impresa di assicurazione e di riassicurazione; — intermediario assicurativo, intermediario riassicurativo e intermediario assicurativo a titolo accessorio; — ente pensionistico aziendale o professionale; — agenzia di rating del credito; — amministratore di indici di riferimento critici; — fornitore di servizi di crowdfunding; — repertorio di dati sulle cartolarizzazioni.
1.5. Denominazione dell'entità finanziaria interessata	Denominazione giuridica completa dell'entità finanziaria interessata dall'incidente grave connesso alle TIC e tenuta a segnalarlo alla propria autorità competente a norma dell'articolo 19 del regolamento (UE) 2022/2554. In caso di segnalazione aggregata: a) elenco di tutte le denominazioni delle entità finanziarie interessate dall'incidente grave connesso alle TIC, separate da un punto e virgola; b) il fornitore terzo che trasmette una notifica o una relazione in merito a un incidente grave in forma aggregata come indicato all'articolo 7 del presente regolamento è tenuto a elencare le denominazioni di tutte le entità finanziarie interessate dall'incidente, separate da un punto e virgola.	Sì, se l'entità finanziaria interessata dall'incidente è diversa dall'entità che trasmette la segnalazione e in caso di segnalazione aggregata.	Sì, se l'entità finanziaria interessata dall'incidente è diversa dall'entità che trasmette la segnalazione e in caso di segnalazione aggregata.	Sì, se l'entità finanziaria interessata dall'incidente è diversa dall'entità che trasmette la segnalazione e in caso di segnalazione aggregata.	Alfanumerico
1.6. Codice LEI dell'entità finanziaria interessata	Identificativo della persona giuridica (*Legal Entity Identifier*, LEI) dell'entità finanziaria interessata dall'incidente grave connesso alle TIC assegnato conformemente alle norme dell'Organizzazione internazionale per la standardizzazione. In caso di segnalazione aggregata: a) un elenco di tutti i codici LEI delle entità finanziarie interessate dall'incidente grave connesso alle TIC, separati da un punto e virgola;	Sì, se l'entità finanziaria interessata dall'incidente grave connesso alle TIC è diversa	Sì, se l'entità finanziaria interessata dall'incidente grave connesso alle TIC è diversa dall'entità che	Sì, se l'entità finanziaria interessata dall'incidente grave connesso alle TIC è	Codice unico di 20 caratteri alfanumerici, basato sulla norma ISO 17442-1:2020

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	b) il fornitore terzo che trasmette una notifica o una relazione in merito a un incidente grave in forma aggregata come indicato all'articolo 7 del presente regolamento è tenuto a elencare i codici LEI di tutte le entità finanziarie interessate dall'incidente, separati da un punto e virgola. L'ordine di presentazione dei codici LEI e delle denominazioni delle entità finanziarie è identico.	dall'entità che trasmette la segnalazione e in caso di segnalazione aggregata.	trasmette la segnalazione e in caso di segnalazione aggregata.	diversa dall'entità che trasmette la segnalazione e in caso di segnalazione aggregata.	
1.7. Nome del referente principale	Nome e cognome del referente principale dell'entità finanziaria. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il nome del referente principale dell'entità che trasmette la segnalazione aggregata.	Sì	Sì	Sì	Alfanumerico
1.8. E-mail: del referente principale	Indirizzo di posta elettronica del referente principale che può essere utilizzato dall'autorità competente per le comunicazioni successive. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, l'indirizzo di posta elettronica del referente principale dell'entità che trasmette la segnalazione aggregata.	Sì	Sì	Sì	Alfanumerico
1.9. Telefono del referente principale	Numero di telefono del referente principale che può essere utilizzato dall'autorità competente per le comunicazioni successive. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il numero di telefono del referente principale dell'entità che trasmette la segnalazione aggregata. Indicare il numero di telefono inserendo tutti i prefissi internazionali (ad esempio +33XXXXXXXXX).	Sì	Sì	Sì	Alfanumerico
1.10. Nome del secondo referente	Nome e cognome del secondo referente o nome del gruppo responsabile dell'entità finanziaria o dell'entità che trasmette la segnalazione per conto dell'entità finanziaria.	Sì	Sì	Sì	Alfanumerico
1.11. E-mail: del secondo referente	Indirizzo di posta elettronica del secondo referente o indirizzo di posta elettronica funzionale del gruppo che può essere utilizzato dall'autorità competente per le comunicazioni successive.	Sì	Sì	Sì	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
1.12. Telefono del secondo referente	Numero di telefono del secondo referente, o di un gruppo, che può essere utilizzato dall'autorità competente per le comunicazioni successive. Indicare il numero di telefono inserendo tutti i prefissi internazionali (ad esempio +33xxxxxxxxx).	Sì	Sì	Sì	Alfanumerico
1.13. Denominazione dell'impresa madre capogruppo	Denominazione dell'impresa madre capogruppo del gruppo cui appartiene l'entità finanziaria interessata, se del caso.	Sì, se l'entità finanziaria appartiene a un gruppo.	Sì, se l'entità finanziaria appartiene a un gruppo.	Sì, se l'entità finanziaria appartiene a un gruppo.	Alfanumerico
1.14. Codice LEI dell'impresa madre capogruppo	Codice LEI dell'impresa madre capogruppo del gruppo cui appartiene l'entità finanziaria interessata, se del caso. Assegnato conformemente alle norme dell'Organizzazione internazionale per la standardizzazione.	Sì, se l'entità finanziaria appartiene a un gruppo.	Sì, se l'entità finanziaria appartiene a un gruppo.	Sì, se l'entità finanziaria appartiene a un gruppo.	Codice unico di 20 caratteri alfanumerici, basato sulla norma ISO 17442-1:2020.
1.15. Valuta della segnalazione	Valuta utilizzata per la segnalazione dell'incidente.	Sì	Sì	Sì	Scelta compilata utilizzando i codici valuta ISO 4217
Contenuto della notifica iniziale					
2.1. Codice di riferimento dell'incidente assegnato dall'entità finanziaria	Codice di riferimento unico emesso dall'entità finanziaria che identifica inequivocabilmente l'incidente grave connesso alle TIC. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il codice di riferimento dell'incidente assegnato dal fornitore terzo.	Sì	Sì	Sì	Alfanumerico
2.2. Data e ora di individuazione dell'incidente connesso alle TIC	Data e ora in cui l'entità finanziaria è venuta a conoscenza dell'incidente connesso alle TIC. Per gli incidenti ricorrenti, data e ora in cui è stato individuato l'ultimo incidente connesso alle TIC.	Sì	Sì	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)

Campo di dati		Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
2.3.	Data e ora della classificazione dell'incidente come grave	Data e ora in cui l'incidente connesso alle TIC è stato classificato come grave secondo i criteri di classificazione stabiliti nel regolamento delegato (UE) 2024/1772.	Sì	Sì	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)
2.4.	Descrizione dell'incidente connesso alle TIC	Descrizione degli aspetti più rilevanti dell'incidente grave connesso alle TIC. Le entità finanziarie forniscono una panoramica di alto livello delle informazioni seguenti, quali possibili cause, impatti immediati, sistemi interessati ecc. Le entità finanziarie indicano altresì, se noto o ragionevolmente previsto, se l'incidente riguarda fornitori terzi o altre entità finanziarie, il tipo di fornitore o di entità finanziaria, il loro nome, i rispettivi codici identificativi e il tipo di codice identificativo (ad esempio LEI o EUID). Nelle relazioni successive il contenuto del campo può evolvere nel tempo in modo da rispecchiare la comprensione costante dell'incidente connesso alle TIC e descrivere qualsiasi altra informazione pertinente sull'incidente connesso alle TIC non rilevata dai campi di dati, comprese la valutazione interna della gravità da parte dell'entità finanziaria (ad esempio molto bassa, bassa, media, elevata, molto elevata) e un'indicazione del livello e del nome delle strutture decisionali di alto livello coinvolte nella risposta all'incidente connesso alle TIC.	Sì	Sì	Sì	Alfanumerico
2.5.	Criteri di classificazione che hanno determinato la segnalazione dell'incidente	I criteri di classificazione di cui al regolamento delegato (UE) 2024/1772 che hanno determinato la qualificazione dell'incidente connesso alle TIC come grave e la successiva notifica e segnalazione. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, i criteri di classificazione che hanno determinato la qualificazione dell'incidente connesso alle TIC come grave per almeno una o più entità finanziarie.	Sì	Sì	Sì	Selezionare (scelta multipla): — clienti, controparti finanziarie e transazioni interessati; — impatto reputazionale; — durata e periodo di inattività del servizio; — estensione geografica; — perdite di dati; — servizi critici colpiti; — impatto economico.
2.6.	Soglie di rilevanza per il criterio di classificazione «Estensione geografica»	Stati membri del SEE interessati dall'incidente grave connesso alle TIC. Nel valutare l'impatto dell'incidente grave connesso alle TIC in altri Stati membri, le entità finanziarie tengono conto degli articoli 4 e 12 del regolamento delegato (UE) 2024/1772.	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Scelta (multipla) compilata utilizzando il codice ISO 3166 ALPHA-2 dei paesi interessati

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
2.7. Constatazione dell'incidente grave connesso alle TIC	Indicare il modo in cui è stato constatato l'incidente grave connesso alle TIC.	Sì	Sì	Sì	Selezionare: — sicurezza informatica; — personale; — audit interno; — audit esterno; — clienti; — controparti finanziarie; — fornitore terzo; — autore dell'attacco; — sistemi di monitoraggio; — autorità/agenzia/orga-nismo di contrasto; — altro.
2.8. Indicazione dell'origine dell'incidente presso un fornitore terzo o presso un'altra entità finanziaria	Indicare se l'incidente grave connesso alle TIC ha origine presso un fornitore terzo o presso un'altra entità finanziaria. Le entità finanziarie indicano se l'incidente grave connesso alle TIC ha origine presso un fornitore terzo o presso un'altra entità finanziaria (comprese le entità finanziarie appartenenti allo stesso gruppo dell'entità che effettua la segnalazione) e il nome, il codice identificativo del fornitore terzo o dell'entità finanziaria e il tipo di codice identificativo (ad esempio LEI o EUID).	Sì, se l'incidente ha origine presso un fornitore terzo o presso un'altra entità finanziaria.	Sì, se l'incidente ha origine presso un fornitore terzo o presso un'altra entità finanziaria.	Sì, se l'incidente ha origine presso un fornitore terzo o presso un'altra entità finanziaria.	Alfanumerico
2.9. Attivazione del piano di continuità operativa, se attivato	Indicare l'eventuale attivazione formale delle misure di risposta in materia di continuità operativa dell'entità finanziaria.	Sì	Sì	Sì	Booleano (Sì o No)
2.10. Altre informazioni pertinenti	Qualsiasi altra informazione non contemplata nel modello. Le entità finanziarie che hanno riclassificato un incidente grave connesso alle TIC come non grave descrivono i motivi per cui l'incidente connesso alle TIC non soddisfa e non dovrebbe soddisfare i criteri per essere considerato un incidente grave connesso alle TIC.	Sì, se vi sono altre informazioni non contemplate nel modello o	Sì, se vi sono altre informazioni non contemplate nel modello o se l'incidente	Sì, se vi sono altre informazioni non contemplate nel modello o	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
		se l'incidente grave connesso alle TIC è stato riclassificato come non grave.	grave connesso alle TIC è stato riclassificato come non grave.	se l'incidente grave connesso alle TIC è stato riclassificato come non grave.	
Contenuto della relazione intermedia					
3.1. Codice di riferimento dell'incidente fornito dall'autorità competente	Codice di riferimento unico assegnato dall'autorità competente al momento del ricevimento della notifica iniziale per identificare inequivocabilmente l'incidente grave connesso alle TIC.	No	Sì, se del caso.	Sì, se del caso.	Alfanumerico
3.2. Data e ora in cui si è verificato l'incidente	Data e ora in cui si è verificato l'incidente grave connesso alle TIC, se diverse dal momento in cui l'entità finanziaria è venuta a conoscenza dell'incidente grave connesso alle TIC. Per gli incidenti ricorrenti gravi connessi alle TIC, la data e l'ora in cui si è verificato l'ultimo incidente grave connesso alle TIC.	No	Sì	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)
3.3. Data e ora di ripristino dei servizi, delle attività o delle operazioni	Indicare la data e l'ora del ripristino dei servizi, delle attività o delle operazioni interessati dall'incidente grave connesso alle TIC.	No	Sì, se è stato compilato il campo di dati 3.16. «Periodo di inattività del servizio»	Sì, se è stato compilato il campo di dati 3.16. «Periodo di inattività del servizio»	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)
3.4. Numero di clienti interessati	Numero di clienti interessati dall'incidente grave connesso alle TIC che si avvalgono del servizio fornito dall'entità finanziaria. Nella valutazione del numero di clienti interessati, le entità finanziarie tengono conto dell'articolo 1, paragrafo 1, e dell'articolo 9, paragrafo 1, lettera b), del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare il numero effettivo di clienti interessati utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il numero totale di clienti interessati in tutte le entità finanziarie.	No	Sì	Sì	Numero intero

Campo di dati		Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.5.	Percentuale di clienti interessati	Percentuale di clienti interessati dall'incidente grave connesso alle TIC rispetto al numero totale di clienti che si avvalgono del servizio interessato fornito dall'entità finanziaria. Nel caso in cui sia interessato più di un servizio, i servizi sono indicati in forma aggregata. Nella loro valutazione le entità finanziarie tengono conto dell'articolo 1, paragrafo 1, e dell'articolo 9, paragrafo 1, lettera a), del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare la percentuale effettiva di clienti interessati utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, l'entità finanziaria divide la somma di tutti i clienti interessati per il numero totale di clienti di tutte le entità finanziarie interessate.	No	Sì	Sì	Espresso come percentuale, qualsiasi valore fino a un massimo di cinque caratteri numerici compreso al massimo un decimale espresso come percentuale (ad esempio 2,4 invece di 2,4 %). Se il valore ha più di una cifra decimale, le controparti segnalanti arrotondano allo 0,5 superiore.
3.6.	Numero di controparti finanziarie interessate	Numero di controparti finanziarie interessate dall'incidente grave connesso alle TIC che hanno concluso un contratto con l'entità finanziaria. Nel valutare il numero di controparti finanziarie interessate, le entità finanziarie tengono conto dell'articolo 1, paragrafo 2, del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare il numero effettivo di controparti finanziarie interessate utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il numero totale di controparti finanziarie interessate in tutte le entità finanziarie.	No	Sì	Sì	Numero intero

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.7. Percentuale di controparti finanziarie interessate	Percentuale di controparti finanziarie interessate dall'incidente grave connesso alle TIC rispetto al numero totale di controparti finanziarie che hanno concluso un contratto con l'entità finanziaria. Nel valutare la percentuale di controparti finanziarie interessate, le entità finanziarie tengono conto dell'articolo 1, paragrafo 1, e dell'articolo 9, paragrafo 1, lettera c), del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare la percentuale effettiva di controparti finanziarie interessate utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, indicare la somma di tutte le controparti finanziarie interessate divisa per il numero totale di controparti finanziarie di tutte le entità finanziarie interessate.	No	Sì	Sì	Espresso come percentuale, qualsiasi valore fino a un massimo di cinque caratteri numerici compreso al massimo un decimale espresso come percentuale (ad esempio 2,4 invece di 2,4 %). Se il valore ha più di una cifra decimale, le controparti segnalanti arrotondano allo 0,5 superiore.
3.8. Impatto su clienti o controparti finanziarie rilevanti	Qualsiasi impatto individuato sui clienti o controparti finanziarie rilevanti di cui all'articolo 1, paragrafo 3, e all'articolo 9, paragrafo 1, lettera f), del regolamento delegato (UE) 2024/1772.	No	Sì, se è raggiunta la soglia per il criterio «Rilevanza dei clienti e delle controparti finanziarie».	Sì, se è raggiunta la soglia per il criterio «Rilevanza dei clienti e delle controparti finanziarie».	Booleano (Sì o No)
3.9. Numero di transazioni interessate	Numero di transazioni interessate dall'incidente grave connesso alle TIC. Nel valutare l'impatto sulle transazioni, le entità finanziarie tengono conto dell'articolo 1, paragrafo 4, del regolamento delegato (UE) 2024/1772, comprese tutte le transazioni nazionali e transfrontaliere interessate che implicano un importo monetario quando almeno una parte della transazione è effettuata nell'Unione.	No	Sì, se l'incidente ha interessato una qualsiasi transazione.	Sì, se l'incidente ha interessato una qualsiasi transazione.	Numero intero

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	L'entità finanziaria che non è in grado di determinare il numero effettivo di transazioni interessate utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, indicare il numero totale di transazioni interessate in tutte le entità finanziarie.				
3.10. Percentuale di transazioni interessate	Percentuale di transazioni interessate rispetto al numero medio giornaliero di transazioni nazionali e transfrontaliere effettuate dall'entità finanziaria in relazione al servizio interessato. Le entità finanziarie tengono conto dell'articolo 1, paragrafo 4, e dell'articolo 9, paragrafo 1, lettera d), del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare la percentuale effettiva di transazioni interessate utilizza stime. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, l'entità finanziaria somma il numero di tutte le transazioni interessate e divide tale somma per il numero totale di transazioni di tutte le entità finanziarie interessate.	No	Sì, se l'incidente ha interessato una qualsiasi transazione.	Sì, se l'incidente ha interessato una qualsiasi transazione.	Espresso come percentuale, qualsiasi valore fino a un massimo di cinque caratteri numerici compreso al massimo un decimale espresso come percentuale (ad esempio 2,4 invece di 2,4 %). Se il valore ha più di una cifra decimale, le controparti segnalanti arrotondano allo 0,5 superiore.
3.11. Valore delle transazioni interessate	Il valore totale delle transazioni interessate dall'incidente grave connesso alle TIC è valutato conformemente all'articolo 1, paragrafo 4, e all'articolo 9, paragrafo 1, lettera e), del regolamento delegato (UE) 2024/1772. L'entità finanziaria che non è in grado di determinare il valore effettivo delle transazioni interessate utilizza stime basate sui dati disponibili relativi a periodi di riferimento comparabili. L'entità finanziaria indica l'importo monetario come valore positivo. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, il valore totale delle transazioni interessate in tutte le entità finanziarie.	No	Sì, se l'incidente ha interessato una qualsiasi transazione.	Sì, se l'incidente ha interessato una qualsiasi transazione.	Monetario Le entità finanziarie segnalano il punto di dati in unità utilizzando una precisione minima equivalente a migliaia di unità (ad esempio 2,5 anziché 2 500 EUR).

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.12. Informazioni indicanti se i numeri sono effettivi o stimati o se non vi è stato alcun impatto	Indicare se i valori riportati nei campi di dati da 3.4. a 3.11. sono effettivi o stimati o se non vi è stato alcun impatto.	No	Sì	Sì	Selezionare (scelta multipla): — cifre effettive relative ai clienti interessati; — cifre effettive relative alle controparti finanziarie interessate; — cifre effettive relative alle transazioni interessate; — stime dei clienti interessati; — stime delle controparti finanziarie interessate; — stime delle transazioni interessate; — nessun impatto sui clienti; — nessun impatto sulle controparti finanziarie; — nessun impatto sulle transazioni.
3.13. Impatto reputazionale	Informazioni sull'impatto reputazionale derivante dall'incidente grave connesso alle TIC di cui agli articoli 2 e 10 del regolamento delegato (UE) 2024/1772. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, le categorie di impatto reputazionale che si applicano ad almeno un'entità finanziaria.	No	Sì, se è soddisfatto il criterio «Impatto reputazionale».	Sì, se è soddisfatto il criterio «Impatto reputazionale».	Selezionare (scelta multipla): — l'incidente grave connesso alle TIC è stato riportato dai media; — l'incidente grave connesso alle TIC ha dato luogo a ripetuti reclami da parte di diversi clienti o controparti finanziarie in relazione a servizi prestati a diretto contatto con i clienti o a relazioni commerciali critiche; — a seguito dell'incidente grave connesso alle TIC l'entità finanziaria non sarà in grado o potrebbe non essere in grado di soddisfare i requisiti normativi; — a seguito dell'incidente grave connesso alle TIC l'entità finanziaria perderà o potrebbe perdere clienti o controparti finanziarie, con un impatto significativo sulla sua attività.
3.14. Informazioni contestuali sull'impatto reputazionale	Descrizione del modo in cui l'incidente grave connesso alle TIC ha inciso o potrebbe incidere sulla reputazione dell'entità finanziaria, comprese le violazioni del diritto, il mancato rispetto dei requisiti normativi, il numero di reclami dei clienti ecc.	No	Sì, se è soddisfatto il criterio «Impatto reputazionale».	Sì, se è soddisfatto il criterio «Impatto reputazionale».	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	Le informazioni contestuali includono il tipo di media (ad esempio media tradizionali e digitali, blog, piattaforme di streaming) e la copertura mediatica, compresa la portata dei media (locali, nazionali, internazionali). La copertura mediatica in questo contesto non comprende i pochi commenti negativi da parte di follower o di utenti dei social network. L'entità finanziaria indica inoltre se la copertura mediatica ha evidenziato rischi significativi per i suoi clienti in relazione all'incidente grave connesso alle TIC, compreso il rischio di insolvenza dell'entità finanziaria o il rischio di perdita di fondi. Le entità finanziarie indicano inoltre se hanno fornito ai media informazioni che sono servite a mettere al corrente il pubblico in modo affidabile dell'incidente grave connesso alle TIC e delle sue conseguenze. Le entità finanziarie possono inoltre indicare se nei media siano state riportate informazioni false in relazione all'incidente connesso alle TIC, comprese informazioni basate sulla diffusione intenzionale di notizie false da parte degli autori delle minacce, o informazioni che riguardano o si riferiscono alla deturpazione (*defacement*) del sito web dell'entità finanziaria.				
3.15. Durata dell'incidente	Le entità finanziarie misurano la durata dell'incidente grave connesso alle TIC a partire dal momento in cui l'incidente si è verificato fino al momento in cui è stato risolto. Le entità finanziarie che non sono in grado di determinare il momento in cui si è verificato l'incidente grave connesso alle TIC misurano la durata dell'incidente grave connesso alle TIC a partire dal momento in cui l'entità finanziaria ha individuato l'incidente o, se precedente, dal momento in cui l'entità finanziaria ha registrato l'incidente nei registri di rete o di sistema o in altre fonti di dati. Le entità finanziarie che non sanno ancora quando l'incidente grave connesso alle TIC sarà risolto applicano stime. Il valore è espresso in giorni, ore e minuti. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento e qualora siano presenti differenze tra le entità finanziarie, queste ultime misurano la durata più lunga dell'incidente grave connesso alle TIC.	No	Sì	Sì	GG:HH:MM

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.16. Periodo di inattività del servizio	Il periodo di inattività del servizio misurato dal momento in cui il servizio è totalmente o parzialmente indisponibile per i clienti, le controparti finanziarie o altri utenti interni o esterni fino al momento in cui sono ripristinate le regolari attività o operazioni al livello di servizio fornito prima dell'incidente grave connesso alle TIC. Se il periodo di inattività del servizio causa un ritardo nella fornitura del servizio dopo che sono state ripristinate le regolari attività o operazioni, le entità finanziarie misurano il periodo di inattività dall'inizio dell'incidente grave connesso alle TIC fino al momento della fornitura del servizio che ha subito il ritardo. Le entità finanziarie che non sono in grado di determinare il momento in cui è iniziato il periodo di inattività del servizio misurano tale periodo a partire dal momento in cui l'incidente è stato individuato o, se precedente, dal momento in cui è stato registrato. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento e qualora siano presenti differenze tra le entità finanziarie, queste ultime misurano la durata più lunga del periodo di inattività del servizio.	No	Sì, se l'incidente ha causato un periodo di inattività del servizio.	Sì, se l'incidente ha causato un periodo di inattività del servizio.	GG:HH:MM
3.17. Informazioni indicanti se i numeri relativi alla durata e al periodo di inattività del servizio sono effettivi o stimati.	Indicare se i valori riportati nei campi di dati 3.15 e 3.16 sono effettivi o stimati.	No	Sì, se è soddisfatto il criterio «Durata e periodo di inattività del servizio».	Sì, se è soddisfatto il criterio «Durata e periodo di inattività del servizio».	Selezionare: — cifre effettive; — stime; — cifre effettive e stime; — informazioni non disponibili.
3.18. Tipi di impatto negli Stati membri	Tipo di impatto nei rispettivi Stati membri del SEE. Indicare se l'incidente grave connesso alle TIC ha avuto un impatto in altri Stati membri del SEE (diversi dallo Stato membro dell'autorità competente cui l'incidente è segnalato direttamente), conformemente all'articolo 4 del regolamento delegato (UE) 2024/1772, in particolare per quanto riguarda la rilevanza dell'impatto in relazione ai seguenti soggetti: a) clienti e controparti finanziarie interessati di altri Stati membri; oppure	No	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Selezionare (scelta multipla): — clienti; — controparti finanziarie; — succursale dell'entità finanziaria; — entità finanziarie del gruppo che svolgono attività in altri Stati membri; — infrastrutture dei mercati finanziari; — fornitori terzi che possono essere comuni ad altre entità finanziarie.

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	b) succursali o altre entità finanziarie del gruppo che svolgono attività in altri Stati membri; oppure c) infrastrutture dei mercati finanziari o fornitori terzi che potrebbero avere un impatto su entità finanziarie di altri Stati membri a cui forniscono servizi.				
3.19. Descrizione dell'impatto dell'incidente in altri Stati membri	Descrizione dell'impatto e della gravità dell'incidente grave connesso alle TIC in ciascuno Stato membro interessato, compresa una valutazione dell'impatto e della gravità sui seguenti soggetti: a) clienti; b) controparti finanziarie; c) succursali dell'entità finanziaria; d) altre entità finanziarie del gruppo che svolgono attività in altri Stati membri; e) infrastrutture dei mercati finanziari; f) fornitori terzi che possono essere comuni ad altre entità finanziarie, se del caso, in altri Stati membri.	No	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Sì, se è raggiunta la soglia per il criterio «Estensione geografica».	Alfanumerico
3.20. Soglie di rilevanza per il criterio di classificazione «Perdite di dati»	Tipo di perdite di dati derivanti dall'incidente grave connesso alle TIC, in relazione alla disponibilità, autenticità, integrità e riservatezza dei dati. Nella loro valutazione le entità finanziarie tengono conto degli articoli 5 e 13 del regolamento delegato (UE) 2024/1772. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, le perdite di dati che interessano almeno un'entità finanziaria.	No	Sì, se è soddisfatto il criterio «Perdite di dati».	Sì, se è soddisfatto il criterio «Perdite di dati».	Selezionare (scelta multipla): — disponibilità; — autenticità; — integrità; — riservatezza.
3.21. Descrizione delle perdite di dati	Descrizione dell'impatto dell'incidente grave connesso alle TIC sulla disponibilità, autenticità, integrità e riservatezza dei dati critici conformemente agli articoli 5 e 13 del regolamento delegato (UE) 2024/1772. Informazioni in merito all'impatto sulla realizzazione degli obiettivi commerciali dell'entità finanziaria o sul rispetto dei requisiti normativi. Nell'ambito delle informazioni fornite, le entità finanziarie indicano se i dati interessati sono dati dei clienti, dati di altre entità (ad esempio controparti finanziarie) o dati dell'entità finanziaria stessa.	No	Sì, se è soddisfatto il criterio «Perdite di dati».	Sì, se è soddisfatto il criterio «Perdite di dati».	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	L'entità finanziaria può anche indicare il tipo di dati coinvolti nell'incidente, in particolare se i dati sono riservati e quale tipo di riservatezza è stato coinvolto (ad esempio riservatezza commerciale/aziendale, dati personali, segreto professionale: segreto bancario, segreto assicurativo, segreto dei servizi di pagamento ecc.). Le informazioni possono includere anche i possibili rischi associati alle perdite di dati, ad esempio se i dati interessati dall'incidente possano essere utilizzati per identificare individui e potrebbero essere utilizzati dall'autore della minaccia per ottenere crediti o prestiti senza il loro consenso, per condurre attacchi di spear phishing e per divulgare informazioni pubblicamente. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, una descrizione generale dell'impatto dell'incidente sulle entità finanziarie interessate. Qualora vi siano differenze di impatto, la descrizione dell'impatto indica chiaramente l'impatto specifico sulle diverse entità finanziarie.				
3.22. Criterio di classificazione «Servizi critici colpiti»	Informazioni relative al criterio «Servizi critici colpiti». Nella loro valutazione le entità finanziarie tengono conto dell'articolo 6 del regolamento delegato (UE) 2024/1772, comprese le informazioni riguardanti: — i servizi o le attività interessati che richiedono l'autorizzazione, la registrazione o che sono sottoposti a vigilanza da parte delle autorità competenti; oppure — i servizi TIC o i sistemi informatici e di rete a supporto di funzioni essenziali o importanti dell'entità finanziaria; nonché — la natura dell'accesso doloso e non autorizzato ai sistemi informatici e di rete dell'entità finanziaria. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, l'impatto sui servizi critici che si applica ad almeno un'entità finanziaria.	No	Sì	Sì	Alfanumerico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.23. Tipo di incidente	Classificazione degli incidenti per tipo.	No	Sì	Sì	Selezionare (scelta multipla): — connesso alla cibersicurezza; — malfunzionamento del processo; — avaria del sistema; — eventi esterni; — connesso ai pagamenti; — altro (precisare).
3.24. Altri tipi di incidenti	Altri tipi di incidenti connessi alle TIC: le entità finanziarie che hanno selezionato «altro» tra i tipi di incidente nel campo di dati 3.23 precisano il tipo di incidente connesso alle TIC.	No	Sì, se tra i tipi di incidente nel campo di dati 3.23 si è selezionato «altro».	Sì, se tra i tipi di incidente nel campo di dati 3.23 si è selezionato «altro».	Alfanumerico
3.25. Minacce e tecniche utilizzate dall'autore della minaccia	Indicare le minacce e le tecniche utilizzate dall'autore della minaccia, tra cui: a) ingegneria sociale, compreso il phishing; b) attacco Distributed Denial of Service (DDoS); c) usurpazione di identità; d) cifratura dei dati per l'impatto, compreso il ransomware; e) dirottamento di risorse; f) estrapolazione e manipolazione dei dati, esclusa l'usurpazione di identità; g) distruzione dei dati; h) defacement; i) attacco alla catena di approvvigionamento; j) altro (precisare).	No	Sì, se il tipo di incidente connesso alle TIC è «connesso alla cibersicurezza» nel campo 3.23.	Sì, se il tipo di incidente connesso alle TIC è «connesso alla cibersicurezza» nel campo 3.23.	Selezionare (scelta multipla): — ingegneria sociale (compreso il phishing); — attacco Distributed Denial of Service (DDoS); — usurpazione di identità; — cifratura dei dati per l'impatto, compreso il ransomware; — dirottamento di risorse; — estrapolazione e manipolazione dei dati, compresa l'usurpazione di identità; — distruzione dei dati; — defacement; — attacco alla catena di approvvigionamento; — altro (precisare).
3.26. Altri tipi di tecniche	Altri tipi di tecniche Le entità finanziarie che hanno selezionato «altro» tra i tipi di tecniche nel campo di dati 3.25 precisano il tipo di tecnica.	No	Sì, se tra i tipi di tecniche nel campo di dati 3.25 si è selezionato «altro».	Sì, se tra i tipi di tecniche nel campo di dati 3.25 si è selezionato «altro».	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.27. Informazioni sulle aree funzionali interessate e sui processi commerciali interessati	Indicazione delle aree funzionali e dei processi commerciali interessati dall'incidente, compresi prodotti e servizi. Le aree funzionali comprendono, tra l'altro: a) marketing e sviluppo aziendale; b) servizio clienti; c) gestione dei prodotti; d) conformità alla normativa; e) gestione del rischio; f) finanza e contabilità; g) risorse umane e servizi generali; h) tecnologie dell'informazione; I processi commerciali comprendono, tra l'altro: — informazione sui conti; — servizi attuariali; — convenzionamento di operazioni di pagamento; — autenticazione/autorizzazione; — autorità — inserimento (on-boarding) di clienti; — gestione delle prestazioni; — gestione dei pagamenti delle prestazioni; — acquisto e vendita di pacchetti di polizze assicurative tra assicurazioni; — pagamenti con carta; — gestione di cassa; — deposito o prelievo di contanti; — gestione dei sinistri; — procedura di sinistro assicurativo; — compensazione; — prestiti a conglomerati di imprese; — assicurazioni collettive; — bonifici; — custodia di attivi; — acquisizione di clienti; — inserimento dati; — elaborazione dati; — addebiti diretti; — assicurazioni per l'esportazione; — conclusione di transazioni/operazioni; — collocamento di strumenti finanziari; — contabilità dei fondi;	No	Sì	Sì	Alfanumerico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	— denaro in valuta estera; — consulenza in materia di investimenti; — gestione degli investimenti; — emissione di strumenti di pagamento; — gestione dei prestiti; — processo di pagamento dell'assicurazione vita; — rimessa di denaro; — calcolo dell'attivo netto; — ordine; — disposizione di ordine di pagamento; — sottoscrizione di assicurazioni; — gestione di portafogli; — riscossione dei premi; — ricevimento/trasmissione/esecuzione; — riassicurazione; — liquidazione; — monitoraggio delle transazioni. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, le aree funzionali e i processi commerciali che sono stati interessati in almeno un'entità finanziaria.				
3.28. Componenti infrastrutturali interessate che sostengono i processi commerciali	Indicare se le componenti infrastrutturali (server, sistemi operativi, software, server applicativi, middleware, componenti di rete, altri) che sostengono i processi commerciali sono state interessate dall'incidente grave connesso alle TIC.	No	Sì	Sì	Selezionare: — Sì — No — Informazioni non disponibili
3.29. Informazioni sulle componenti infrastrutturali interessate che sostengono i processi commerciali	Descrizione dell'impatto dell'incidente grave connesso alle TIC sulle componenti infrastrutturali che sostengono i processi commerciali, compresi hardware e software. L'hardware comprende server, computer, centri dati, commutatori, router, hub. Il software comprende sistemi operativi, applicazioni, banche dati, strumenti di sicurezza, componenti di rete, altro, precisare. Fornire la descrizione o il nome delle componenti o dei sistemi infrastrutturali interessati e, se disponibili, indicare: a) informazioni sulla versione; b) se si tratta di un'infrastruttura interna/parzialmente esternalizzata/interamente esternalizzata, il nome del fornitore terzo;	No	Sì, se l'incidente ha interessato componenti infrastrutturali che sostengono i processi commerciali.	Sì, se l'incidente ha interessato componenti infrastrutturali che sostengono i processi commerciali.	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	c) se l'infrastruttura è utilizzata o condivisa da più funzioni operative; d) i meccanismi messi in atto in termini di resilienza/continuità/ripristino/sostituibilità.				
3.30. Impatto sugli interessi finanziari dei clienti	Indicare se l'incidente grave connesso alle TIC ha inciso sugli interessi finanziari dei clienti.	No	Sì	Sì	Selezionare: — Sì — No — Informazioni non disponibili
3.31. Segnalazione ad altre autorità	Specificare quali autorità sono state informate dell'incidente grave connesso alle TIC. Tenendo conto delle differenze derivanti dalla legislazione nazionale degli Stati membri, il concetto di autorità di contrasto è inteso dalle entità finanziarie in senso lato in modo da includere le autorità pubbliche abilitate a perseguire la criminalità informatica, comprese le forze di polizia, le agenzie di contrasto e i pubblici ministeri.	No	Sì	Sì	Selezionare (scelta multipla): — forze di polizia/autorità di contrasto — CSIRT — autorità competente per la protezione dei dati — agenzia nazionale per la cibersicurezza — nessuna — altre (precisare)
3.32. Indicazione delle autorità di «altro» tipo	Specificare quale «altro» tipo di autorità è stato informato dell'incidente grave connesso alle TIC. Se nel campo di dati 3.31 si è selezionato «altro», la descrizione comprende informazioni più dettagliate sull'autorità alla quale l'entità finanziaria ha trasmesso informazioni sull'incidente grave connesso alle TIC.	No	Sì, se l'entità finanziaria ha informato un «altro» tipo di autorità in merito all'incidente grave connesso alle TIC.	Sì, se l'entità finanziaria ha informato un «altro» tipo di autorità in merito all'incidente grave connesso alle TIC.	Alfanumerico
3.33. Azioni/misure temporanee adottate o previste per effettuare il ripristino a seguito dell'incidente	Indicare se l'entità finanziaria ha attuato (o prevede di attuare) eventuali azioni temporanee che sono state adottate (o di cui è prevista l'adozione) per effettuare il ripristino a seguito dell'incidente grave connesso alle TIC.	No	Sì	Sì	Booleano (Sì o No)

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
3.34. Descrizione di eventuali azioni e misure temporanee adottate o previste per effettuare il ripristino a seguito dell'incidente	Le informazioni descrivono le azioni immediate adottate, compreso l'isolamento dell'incidente a livello di rete, l'attivazione delle procedure di risoluzione, il blocco delle porte USB, l'attivazione del sito di ripristino in caso di disastro e qualsiasi altro controllo di sicurezza supplementare temporaneamente messo in atto. Le entità finanziarie indicano la data e l'ora di attuazione delle azioni temporanee e la data prevista di ritorno al sito primario. Per eventuali azioni temporanee che non sono state attuate ma sono ancora pianificate, indicare la data entro la quale è prevista la loro attuazione. Se non sono state adottate azioni/misure temporanee, indicarne il motivo.	No	Sì, se sono state adottate o si prevede di adottare azioni/misure temporanee (campo di dati 3.33).	Sì, se sono state adottate o si prevede di adottare azioni/misure temporanee (campo di dati 3.33).	Alfanumerico
3.35. Indicatori di compromissione	Informazioni relative all'incidente grave connesso alle TIC che possono contribuire a individuare attività dolose all'interno di un sistema informatico o di rete (indicatori di compromissione o IoC), se del caso. Il campo si applica solo alle entità finanziarie che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([1]) e alle entità finanziarie identificate come soggetti essenziali o importanti ai sensi delle norme nazionali che recepiscono l'articolo 3 della direttiva (UE) 2022/2555, se del caso. Gli IoC forniti dall'entità finanziaria comprendono le categorie di dati seguenti: a) indirizzi IP; b) indirizzi URL; c) domini; d) hash dei file; e) dati del malware (nome del malware, nomi dei file e loro ubicazione, chiavi di registro specifiche associate all'attività di malware); f) dati relativi alle attività di rete (porte, protocolli, indirizzi, referrer, programmi utente, header, log specifici o schemi distintivi nel traffico di rete); g) dati del messaggio di posta elettronica (mittente, destinatario, oggetto, intestazione, contenuto);	No	Sì, se nel campo di dati 3.23 è selezionato come tipo di incidente connesso alla cibersicurezza.	Sì, se nel campo di dati 3.23 è selezionato come tipo di incidente connesso alla cibersicurezza.	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	h) richieste DNS e configurazioni dei registri; i) attività dell'account utente (login, attività di account utente privilegiato, privilege escalation); j) traffico delle banche dati (lettura/scrittura), richieste relative allo stesso file. In pratica, questo tipo di informazioni può includere dati relativi, tra l'altro, agli indicatori che descrivono gli schemi nel traffico di rete corrispondenti ad attacchi noti/comunicazioni botnet, indirizzi IP delle macchine infette da malware (bot), dati relativi ai server di «comando e controllo» utilizzati dai malware (solitamente domini o indirizzi IP) e URL relativi a siti di phishing o a siti web osservati che ospitano malware o sfruttano kit.				
Contenuto della relazione finale					
4.1. Classificazione di alto livello delle cause di fondo dell'incidente	Classificazione di alto livello delle cause di fondo dell'incidente grave connesso alle TIC in base ai tipi di incidente, comprese le categorie di alto livello seguenti: a) azioni dolose; b) malfunzionamento del processo; c) avaria/malfunzionamento del sistema; d) errore umano; e) evento esterno.	No	No	Sì	Selezionare (scelta multipla): — azioni dolose; — malfunzionamento del processo; — avaria/malfunzionamento del sistema; — errore umano; — evento esterno.
4.2. Classificazione dettagliata delle cause di fondo dell'incidente	Classificazione dettagliata delle cause di fondo dell'incidente grave connesso alle TIC in base ai tipi di incidente, comprese le categorie dettagliate seguenti collegate alle categorie di alto livello riportate nel campo di dati 4.1. 1. **Azioni dolose** (se selezionato, scegliere una o più delle opzioni seguenti): a) azioni interne intenzionali; b) danni fisici intenzionali/manipolazione/furto; c) azioni fraudolente. 2. **Malfunzionamento del processo** (se selezionato, scegliere una o più delle opzioni seguenti): a) inadeguatezza del monitoraggio o carenza del monitoraggio e del controllo;	No	No	Sì	Selezionare (scelta multipla): — azioni dolose: azioni interne intenzionali; — azioni dolose: danni fisici intenzionali/manipolazione/furto; — azioni dolose: azioni fraudolente; — malfunzionamento del processo: inadeguatezza del monitoraggio o carenza del monitoraggio e del controllo; — malfunzionamento del processo: ruoli e responsabilità insufficienti/poco chiari; — malfunzionamento del processo: malfunzionamento del processo di gestione dei rischi connessi alle TIC; — malfunzionamento del processo: inadeguatezza o malfunzionamento delle operazioni TIC e delle operazioni di sicurezza TIC;

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	b) ruoli e responsabilità insufficienti/poco chiari; c) malfunzionamento del processo di gestione dei rischi connessi alle TIC; d) inadeguatezza o malfunzionamento delle operazioni TIC e delle operazioni di sicurezza TIC; e) inadeguatezza o carenza della gestione dei progetti TIC; f) inadeguatezza delle politiche, delle procedure e della documentazione interne; g) inadeguatezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi TIC; h) altro (precisare). 3. **Avaria/malfunzionamento del sistema** (se selezionato, scegliere una o più delle opzioni seguenti): a) capacità e prestazioni dell'hardware: incidenti gravi connessi alle TIC causati da risorse hardware che si dimostrano inadeguate in termini di capacità o prestazioni per soddisfare gli obblighi legislativi applicabili; b) manutenzione dell'hardware: incidenti gravi connessi alle TIC derivanti da una manutenzione inadeguata o insufficiente dei componenti hardware, eccetto «obsolescenza/invecchiamento dell'hardware»; c) obsolescenza/invecchiamento dell'hardware: questo tipo di causa di fondo riguarda gli incidenti gravi connessi alle TIC derivanti da componenti hardware obsoleti o invecchiati; d) compatibilità/configurazione del software: incidenti gravi connessi alle TIC causati da componenti software incompatibili con altre configurazioni di software o sistemi, compresi gli incidenti gravi connessi alle TIC derivanti da conflitti di software, impostazioni errate o parametri configurati non correttamente che incidono sulla funzionalità complessiva del sistema; e) prestazioni del software: incidenti gravi connessi alle TIC derivanti da componenti software che presentano prestazioni insufficienti o inefficienze, per motivi diversi da quelli specificati alla voce «Compatibilità/ configurazione del software», compresi gli incidenti gravi connessi alle TIC causati da tempi di risposta lenti, consumo eccessivo di risorse o esecuzione inefficiente delle interrogazioni che incidono sulle prestazioni del software o del sistema;				— malfunzionamento del processo: inadeguatezza o carenza della gestione dei progetti TIC; — malfunzionamento del processo: inadeguatezza delle politiche, delle procedure e della documentazione interne; — malfunzionamento del processo: inadeguatezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi TIC; — malfunzionamento del processo: altro (precisare); — avaria del sistema: capacità e prestazioni dell'hardware; — avaria del sistema: manutenzione dell'hardware; — avaria del sistema: obsolescenza/ invecchiamento dell'hardware; — avaria del sistema: compatibilità/ configurazione del software; — avaria del sistema: prestazioni del software; — avaria del sistema: configurazione della rete; — avaria del sistema: danni fisici; — avaria del sistema: altro (precisare); — errore umano: omissione; - — errore umano: errore; — errore umano: competenze e conoscenze; — errore umano: risorse umane insufficienti; — errore umano: cattiva comunicazione; — errore umano: altro (precisare); — evento esterno: calamità naturali/forza maggiore; — evento esterno: disfunzioni di terzi; — evento esterno: altro (precisare).

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	f) configurazione della rete: incidenti gravi connessi alle TIC derivanti da impostazioni o infrastrutture di rete non corrette o mal configurate, compresi gli incidenti gravi connessi alle TIC causati da errori di configurazione della rete, problemi di instradamento, configurazioni non corrette del firewall o altri problemi legati alla rete che incidono sulla connettività o sulla comunicazione; g) danni fisici: incidenti gravi connessi alle TIC causati da danni fisici alle infrastrutture TIC che provocano guasti del sistema; h) altro (precisare). 4. **Errore umano** (se selezionato, scegliere uno o più degli elementi seguenti): a) omissione (non intenzionale); b) errore; c) competenze e conoscenze: incidenti gravi connessi alle TIC derivanti dalla mancanza di esperienza o competenze nella gestione di sistemi o processi TIC che possono essere causati da una formazione inadeguata, conoscenze insufficienti o carenze delle competenze necessarie per svolgere compiti specifici o affrontare sfide tecniche; d) risorse umane insufficienti: incidenti gravi connessi alle TIC causati dalla mancanza delle risorse necessarie, tra cui hardware, software, infrastrutture o personale, comprese le situazioni in cui l'insufficienza delle risorse comporta inefficienze operative, guasti del sistema o incapacità di soddisfare le esigenze commerciali; e) cattiva comunicazione; f) altro (precisare). 5. **Evento esterno** (se selezionato, scegliere una o più delle opzioni seguenti): a) calamità naturali/forza maggiore; b) disfunzioni di terzi;				

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	c) altro (precisare). Le entità finanziarie tengono conto del fatto che, per gli incidenti ricorrenti gravi connessi alle TIC, si tiene conto della causa di fondo specifica apparente dell'incidente e non delle categorie generali incluse in questo campo.				
4.3. Ulteriore classificazione delle cause di fondo dell'incidente	Ulteriore classificazione delle cause di fondo dell'incidente grave connesso alle TIC in base al tipo di incidente, comprese le ulteriori categorie di classificazione seguenti collegate alle categorie dettagliate che devono essere segnalate nel campo di dati 4.2. Il campo è obbligatorio per la relazione finale se nel campo di dati 4.2 sono riportate categorie specifiche che richiedono un ulteriore livello di dettaglio. 2 a) **Inadeguatezza o carenza del monitoraggio e del controllo:** a) monitoraggio del rispetto delle politiche; b) monitoraggio di fornitori terzi di servizi; c) monitoraggio e verifica della correzione delle vulnerabilità; d) gestione dell'identità e dell'accesso; e) cifratura e crittografia; f) registrazione. 2 c) **Malfunzionamento del processo di gestione dei rischi connessi alle TIC:** a) mancata specificazione di livelli accurati di tolleranza al rischio; b) valutazioni insufficienti della vulnerabilità e delle minacce; c) misure di trattamento dei rischi inadeguate; d) cattiva gestione dei rischi connessi alle TIC residui. 2 d) **Inadeguatezza o malfunzionamento delle operazioni TIC e delle operazioni di sicurezza TIC:** a) gestione delle vulnerabilità e delle patch; b) gestione delle modifiche; c) gestione della capacità e delle prestazioni; d) gestione delle risorse TIC e classificazione delle informazioni;	No	No	Sì	Selezionare (scelta multipla): — monitoraggio del rispetto delle politiche; — monitoraggio di fornitori terzi di servizi; — monitoraggio e verifica della correzione delle vulnerabilità; — gestione dell'identità e dell'accesso; — cifratura e crittografia; — registrazione; — mancata specificazione di livelli accurati di tolleranza al rischio; — valutazioni insufficienti della vulnerabilità e delle minacce; — misure di trattamento dei rischi inadeguate; — cattiva gestione dei rischi connessi alle TIC residui; — gestione delle vulnerabilità e delle patch; — gestione delle modifiche; — gestione della capacità e delle prestazioni; — gestione delle risorse TIC e classificazione delle informazioni; — backup e ripristino; — trattamento degli errori; — inadeguatezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi TIC; — inadeguatezza o malfunzionamento dei test del software.

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	e) backup e ripristino; f) trattamento degli errori. 2 g) **Inadeguatezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi TIC:** a) inadeguatezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi TIC; b) inadeguatezza dei test del software o malfunzionamento dei test del software.				
4.4. Altri tipi di cause di fondo	Le entità finanziarie che hanno selezionato «altro» tra i tipi di cause di fondo nel campo di dati 4.2 precisano gli altri tipi di tipi di cause di fondo.	No	No	Sì, se tra i tipi di cause di fondo nel campo di dati 4.2 si è selezionato «altro».	Alfanumerico
4.5. Informazioni sulle cause di fondo dell'incidente	Descrizione della sequenza di eventi all'origine dell'incidente grave connesso alle TIC e descrizione del modo in cui l'incidente grave connesso alle TIC ha una causa di fondo apparente analoga se tale incidente è classificato come incidente ricorrente, compresa una descrizione concisa di tutti i motivi sottostanti e dei fattori primari che hanno contribuito al verificarsi dell'incidente grave connesso alle TIC. In caso di azioni dolose, descrizione del modus operandi dell'azione dolosa, comprese le tattiche, le tecniche e le procedure utilizzate, nonché il vettore di ingresso dell'incidente grave connesso alle TIC, compresa una descrizione delle indagini e delle analisi che hanno portato all'individuazione delle cause di fondo, se del caso.	No	No	Sì	Alfanumerico
4.6. Risoluzione dell'incidente	Ulteriori informazioni sulle azioni/misure adottate/previste per risolvere in modo definitivo l'incidente grave connesso alle TIC e per evitare che tale incidente si ripeta. Insegnamenti tratti dall'incidente grave connesso alle TIC.	No	No	Sì	Alfanumerico

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	La descrizione contiene i punti indicati di seguito. 1. **Descrizione delle azioni di risoluzione:** a) azioni adottate per risolvere in modo definitivo l'incidente grave connesso alle TIC (escluse le azioni temporanee); b) per ciascuna azione adottata, indicare il potenziale coinvolgimento di un fornitore terzo e dell'entità finanziaria; c) indicare se le procedure sono state adattate a seguito dell'incidente grave connesso alle TIC; d) indicare eventuali controlli supplementari messi in atto o previsti con il relativo calendario di attuazione. Potenziali problemi individuati in merito alla solidità dei sistemi informatici interessati/o in termini di procedure o controlli in atto, se del caso. Le entità finanziarie indicano chiaramente in che modo le azioni correttive previste affronteranno le cause di fondo individuate e quando si prevede che l'incidente grave connesso alle TIC sarà risolto in modo definitivo. 2. **Insegnamenti appresi** Le entità finanziarie descrivono i risultati dell'analisi successiva all'incidente.				
4.7. Data e ora in cui è stata affrontata la causa di fondo dell'incidente	Data e ora in cui è stata affrontata la causa di fondo dell'incidente.	No	No	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)
4.8. Data e ora in cui l'incidente è stato risolto	Data e ora in cui l'incidente è stato risolto.	No	No	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
4.9. Indicare se la data di risoluzione definitiva degli incidenti differisce dalla data di attuazione inizialmente prevista	Descrizione del motivo per cui la data di risoluzione definitiva degli incidenti gravi connessi alle TIC è diversa dalla data di attuazione inizialmente prevista, se del caso.	No	No	Sì	Alfanumerico
4.10. Valutazione del rischio per le funzioni essenziali ai fini della risoluzione	Valutazione dell'eventualità che l'incidente grave connesso alle TIC comporti un rischio per le funzioni essenziali ai sensi dell'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE del Parlamento europeo e del Consiglio ([2]). Le entità di cui all'articolo 1, paragrafo 1, della direttiva 2014/59/UE indicano se l'incidente comporta un rischio per le funzioni essenziali ai sensi dell'articolo 2, paragrafo 1, punto 35), della medesima direttiva, e se è segnalato nel modello Z07.01 del regolamento di esecuzione (UE) 2018/1624 della Commissione ([3]) e associato all'entità specifica nel modello Z07.02.	No	No	Sì, se l'incidente comporta un rischio per le funzioni essenziali delle entità finanziarie a norma dell'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE.	Alfanumerico
4.11. Informazioni pertinenti per le autorità di risoluzione	Descrivere se e, in caso affermativo, in che modo l'incidente grave connesso alle TIC ha inciso sulla possibilità di risoluzione dell'entità o del gruppo. Le entità di cui all'articolo 1, paragrafo 1, della direttiva 2014/59/UE comunicano se e, in caso affermativo, in che modo l'incidente grave connesso alle TIC ha inciso sulla possibilità di risoluzione dell'entità o del gruppo. Tali entità indicano inoltre se l'incidente grave connesso alle TIC incide sulla solvibilità o sulla liquidità dell'entità finanziaria e sulla potenziale quantificazione dell'impatto. Tali entità forniscono inoltre informazioni relative all'impatto sulla continuità operativa, all'impatto sulla possibilità di risoluzione dell'entità, a qualsiasi impatto aggiuntivo sui costi e sulle perdite derivanti dall'incidente grave connesso alle TIC, compresa la posizione patrimoniale dell'entità finanziaria, e indicanti se gli accordi contrattuali sull'utilizzo dei servizi TIC sono ancora solidi e pienamente applicabili in caso di risoluzione dell'entità.	No	No	Sì, se l'incidente ha inciso sulla possibilità di risoluzione dell'entità o del gruppo.	Alfanumerico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
4.12. Soglia di rilevanza per il criterio di classificazione «Impatto economico»	Informazioni dettagliate sulle soglie raggiunte alla fine dall'incidente grave connesso alle TIC in relazione al criterio «Impatto economico» di cui agli articoli 7 e 14 del regolamento delegato (UE) 2024/1772.	No	No	Sì	Alfanumerico
4.13. Importo dei costi diretti e indiretti e delle perdite lordi	Importo totale dei costi diretti e indiretti e delle perdite lordi sostenuti dall'entità finanziaria a causa dell'incidente grave connesso alle TIC, compresi: a) l'importo dei fondi o delle attività finanziarie espropriati di cui l'entità finanziaria è responsabile; b) l'importo dei costi per la sostituzione o il trasferimento di software, hardware o infrastrutture; c) l'importo dei costi del personale, compresi i costi associati alla sostituzione o al trasferimento del personale, all'assunzione di personale supplementare, alla remunerazione degli straordinari e al recupero delle competenze perdute o compromesse; d) l'importo delle spese dovute all'inosservanza degli obblighi contrattuali; e) l'importo dei costi di risarcimenti e indennizzi ai clienti; f) l'importo delle perdite dovute a mancati introiti; g) l'importo dei costi associati alla comunicazione interna ed esterna; h) l'importo dei costi di consulenza, compresi i costi associati alla consulenza legale, ai servizi forensi e ai servizi per rimediare all'incidente; i) l'importo di altri costi e perdite, compresi: i) gli oneri diretti, comprese le rettifiche e i costi di transazione, contabilizzati nel conto profitti e perdite e le svalutazioni (*write-down*) dovute all'incidente grave connesso alle TIC; ii) gli accantonamenti o le riserve contabilizzati nel conto profitti e perdite a fronte di probabili perdite connesse all'incidente grave connesso alle TIC;	No	No	Sì	Monetario

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	iii) le *pending losses*, ossia le perdite derivanti da un incidente grave connesso alle TIC che sono temporaneamente iscritte in conti transitori o in sospeso e non sono ancora rispecchiate nel conto profitti e perdite, che dovrebbero essere incluse entro un periodo di tempo proporzionale alla dimensione e all'età della voce in sospeso; iv) i ricavi rilevanti non riscossi, connessi agli obblighi contrattuali con terzi, compresa la decisione di compensare un cliente a seguito dell'incidente grave connesso alle TIC, invece che mediante rimborso o pagamento diretto, mediante una rettifica del ricavo che abolisce o riduce le spese contrattuali per uno specifico periodo di tempo futuro; v) le *timing losses*, se abbracciano più di un esercizio finanziario e danno luogo a rischi giuridici. Nella loro valutazione le entità finanziarie tengono conto dell'articolo 7, paragrafi 1 e 2, del regolamento delegato (UE) 2024/1772. Le entità finanziarie non includono in questo dato recuperi finanziari di alcun tipo. Le entità finanziarie indicano l'importo monetario come valore positivo. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, le entità finanziarie tengono conto dell'importo totale dei costi e delle perdite in tutte le entità finanziarie. Le entità finanziarie segnalano il punto di dati in unità utilizzando una precisione minima equivalente a migliaia di unità.				
4.14. Importo dei recuperi finanziari	Importo totale dei recuperi finanziari. I recuperi finanziari si riferiscono alla perdita originaria causata dall'incidente, indipendentemente dal momento in cui sono ricevuti i recuperi finanziari sotto forma di fondi o afflussi di benefici economici.	No	No	Sì	Monetario Le entità finanziarie segnalano il punto di dati in unità utilizzando una precisione minima equivalente a migliaia di unità.

Campo di dati	Descrizione	Obbligatorio per la notifica iniziale	Obbligatorio per la relazione intermedia	Obbligatorio per la relazione finale	Tipo di campo
	Le entità finanziarie indicano l'importo monetario come valore positivo. In caso di segnalazione aggregata di cui all'articolo 7 del presente regolamento, le entità finanziarie tengono conto dell'importo totale dei recuperi finanziari in tutte le entità finanziarie.				
4.15. Informazioni indicanti se gli incidenti non gravi sono stati ricorrenti	Indicare se più incidenti non gravi connessi alle TIC sono stati ricorrenti e se sono considerati congiuntamente un incidente grave ai sensi dell'articolo 8, paragrafo 2, del regolamento delegato (UE) 2024/1772. Le entità finanziarie indicano se gli incidenti non gravi connessi alle TIC sono stati ricorrenti e se sono considerati congiuntamente un incidente grave connesso alle TIC. Le entità finanziarie indicano inoltre il numero di volte in cui tali incidenti non gravi connessi alle TIC si sono verificati.	No	No	Sì, se l'incidente grave comprende più di un incidente ricorrente non grave.	Alfanumerico
4.16. Data e ora in cui si sono verificati incidenti ricorrenti	Se le entità finanziarie segnalano incidenti ricorrenti connessi alle TIC, la data e l'ora in cui si è verificato il primo incidente connesso alle TIC.	No	No	Sì, in caso di incidenti ricorrenti.	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)

([1]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio (GU L 173 del 12.6.2014, pag. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Regolamento di esecuzione (UE) 2018/1624 della Commissione, del 23 ottobre 2018, che stabilisce norme tecniche di attuazione per quanto riguarda le procedure e i moduli e modelli standard per la presentazione di informazioni ai fini dei piani di risoluzione per gli enti creditizi e le imprese di investimento ai sensi della direttiva 2014/59/UE del Parlamento europeo e del Consiglio e che abroga il regolamento di esecuzione (UE) 2016/1066 della Commissione (GU L 277 del 7.11.2018, pag. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ALLEGATO III

MODELLI PER LA NOTIFICA DELLE MINACCE INFORMATICHE SIGNIFICATIVE

Numero del campo	Campo di dati	
1	Denominazione dell'entità che trasmette la notifica	
2	Codice identificativo dell'entità che trasmette la notifica	
3	Tipo di entità finanziaria che trasmette la notifica	
4	Denominazione dell'entità finanziaria	
5	Codice LEI dell'entità finanziaria	
6	Nome del referente principale	
7	E-mail: del referente principale	
8	Telefono del referente principale	
9	Nome del secondo referente	
10	E-mail: del secondo referente	
11	Telefono del secondo referente	
12	Data e ora di individuazione della minaccia informatica	
13	Descrizione della minaccia informatica significativa	
14	Informazioni sull'impatto potenziale	
15	Criteri di classificazione del potenziale incidente	
16	Stato della minaccia informatica	
17	Azioni adottate per prevenire il concretizzarsi della minaccia	
18	Notifica ad altri portatori di interessi	
19	Indicatori di compromissione	
20	Altre informazioni pertinenti	

ALLEGATO IV

GLOSSARIO DEI DATI E ISTRUZIONI PER LA NOTIFICA DELLE MINACCE INFORMATICHE SIGNIFICATIVE

Campo di dati	Descrizione	Campo obbligatorio	Tipo di campo
1. Denominazione dell'entità che trasmette la notifica	Denominazione giuridica completa dell'entità che trasmette la notifica.	Sì	Alfanumerico
2. Codice identificativo dell'entità che trasmette la notifica	Codice identificativo dell'entità che trasmette la notifica. Se la notifica/relazione è trasmessa da entità finanziarie, il codice identificativo è un identificativo della persona giuridica (*Legal Entity Identifier*, LEI), che è un codice unico composto da 20 caratteri alfanumerici, basato sulla norma ISO 17442-1:2020. Se un fornitore terzo trasmette una segnalazione per un'entità finanziaria può utilizzare un codice identificativo come specificato nelle norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.	Sì	Alfanumerico
3. Tipo di entità finanziaria che trasmette la segnalazione	Tipo di entità di cui all'articolo 2, paragrafo 1, lettere da a) a t), del regolamento (UE) 2022/2554 che trasmette la segnalazione.	Sì, se la segnalazione non è trasmessa direttamente dall'entità finanziaria interessata.	Selezionare (scelta multipla): — ente creditizio; — istituto di pagamento; — istituto di pagamento esentato; — prestatore di servizi di informazione sui conti; — istituto di moneta elettronica; — istituto di moneta elettronica esentato; — impresa di investimento; — fornitore di servizi per le cripto-attività; — emittente di token collegati ad attività; — depositario centrale di titoli; — controparte centrale; — sede di negoziazione; — repertorio di dati sulle negoziazioni; — gestore di fondi di investimento alternativi; — società di gestione; — fornitore di servizi di comunicazione dati;

Campo di dati		Descrizione	Campo obbligatorio	Tipo di campo
				— impresa di assicurazione e di riassicurazione; — intermediario assicurativo, intermediario riassicurativo e intermediario assicurativo a titolo accessorio; — ente pensionistico aziendale o professionale; — agenzia di rating del credito; — amministratore di indici di riferimento critici; — fornitore di servizi di crowdfunding; — repertorio di dati sulle cartolarizzazioni.
4.	Denominazione dell'entità finanziaria	Denominazione giuridica completa dell'entità finanziaria che notifica la minaccia informatica significativa.	Sì, se l'entità finanziaria è diversa dall'entità che trasmette la notifica.	Alfanumerico
5.	Codice LEI dell'entità finanziaria	Identificativo della persona giuridica (*Legal Entity Identifier*, LEI) dell'entità finanziaria che notifica la minaccia informatica significativa, assegnato conformemente alle norme dell'Organizzazione internazionale per la standardizzazione.	Sì, se l'entità finanziaria che notifica la minaccia informatica significativa è diversa dall'entità che trasmette la segnalazione.	Codice unico di 20 caratteri alfanumerici, basato sulla norma ISO 17442-1:2020
6.	Nome del referente principale	Nome e cognome del referente principale dell'entità finanziaria.	Sì	Alfanumerico
7.	E-mail: del referente principale	Indirizzo di posta elettronica del referente principale che può essere utilizzato dall'autorità competente per le comunicazioni successive.	Sì	Alfanumerico
8.	Telefono del referente principale	Numero di telefono del referente principale che può essere utilizzato dall'autorità competente per le comunicazioni successive. Indicare il numero di telefono inserendo tutti i prefissi internazionali (ad esempio +33XXXXXXXXX).	Sì	Alfanumerico
9.	Nome del secondo referente	Nome e cognome del secondo referente dell'entità finanziaria o dell'entità che trasmette la notifica per conto dell'entità finanziaria, se disponibile.	Sì, se sono disponibili il nome e il cognome del secondo referente dell'entità finanziaria o dell'entità che trasmette la notifica per l'entità finanziaria.	Alfanumerico

Campo di dati		Descrizione	Campo obbligatorio	Tipo di campo
10.	E-mail: del secondo referente	Indirizzo di posta elettronica del secondo referente o indirizzo di posta elettronica funzionale del gruppo che può essere utilizzato dall'autorità competente per le comunicazioni successive, se disponibile.	Sì, se è disponibile l'indirizzo di posta elettronica del secondo referente o un indirizzo di posta elettronica funzionale del gruppo che può essere utilizzato dall'autorità competente per le comunicazioni successive.	Alfanumerico
11.	Telefono del secondo referente	Numero di telefono del secondo referente che può essere utilizzato dall'autorità competente per le comunicazioni successive, se disponibile. Indicare il numero di telefono inserendo tutti i prefissi internazionali (ad esempio +33XXXXXXXXX).	Sì, se è disponibile il numero di telefono del secondo referente che può essere utilizzato dall'autorità competente per le comunicazioni successive.	Alfanumerico
12.	Data e ora di individuazione della minaccia informatica	Data e ora in cui l'entità finanziaria è venuta a conoscenza della minaccia informatica significativa.	Sì	UTC secondo la norma ISO 8601 (AAAA-MM-GG T hh: mm:ss)
13.	Descrizione della minaccia informatica significativa	Descrizione degli aspetti più rilevanti della minaccia informatica significativa. Le entità finanziarie forniscono: a) una panoramica di alto livello degli aspetti più rilevanti della minaccia informatica significativa; b) i rischi correlati che ne derivano, comprese le potenziali vulnerabilità dei sistemi dell'entità finanziaria che possono essere sfruttate; c) informazioni sulla probabilità che la minaccia informatica significativa si concretizzi; nonché d) dati sulla fonte di informazioni sulla minaccia informatica.	Sì	Alfanumerico
14.	Informazioni sull'impatto potenziale	Informazioni relative al potenziale impatto della minaccia informatica sull'entità finanziaria, sui suoi clienti o sulle sue controparti finanziarie se la minaccia informatica si fosse concretizzata.	Sì	Alfanumerico
15.	Criteri di classificazione del potenziale incidente	I criteri di classificazione che avrebbero potuto determinare una segnalazione di incidente grave se la minaccia informatica si fosse concretizzata.	Sì	Selezionare (scelta multipla): — clienti, controparti finanziarie e transazioni interessati; — impatto reputazionale; — durata e periodo di inattività del servizio; — estensione geografica; — perdite di dati; — servizi critici colpiti; — impatto economico.

Campo di dati		Descrizione	Campo obbligatorio	Tipo di campo
16.	Stato della minaccia informatica	Informazioni indicanti lo stato della minaccia informatica per l'entità finanziaria e se vi siano stati cambiamenti nell'attività di minaccia. Se la minaccia informatica ha cessato la comunicazione con i sistemi informatici dell'entità finanziaria, lo stato può essere contrassegnato come inattivo. Se l'entità finanziaria dispone di informazioni secondo cui la minaccia rimane attiva nei confronti di altre parti o del sistema finanziario nel suo complesso, lo stato è contrassegnato come attivo.	Sì	Selezionare: — attivo; — inattivo.
17.	Azioni adottate per prevenire il concretizzarsi della minaccia	Informazioni di alto livello sulle azioni adottate dall'entità finanziaria per prevenire il concretizzarsi delle minacce informatiche significative, se del caso.	Sì	Alfanumerico
18.	Notifica ad altri portatori di interessi	Informazioni sulla notifica della minaccia informatica ad altre entità finanziarie o autorità.	Sì, se altre entità finanziarie o autorità sono state informate della minaccia informatica.	Alfanumerico
19.	Indicatori di compromissione	Informazioni relative alla minaccia significativa che possono contribuire a individuare attività dolose all'interno di un sistema informatico o di rete (indicatori di compromesso o IoC), se del caso. Gli IoC forniti dall'entità finanziaria possono includere, tra l'altro, le categorie di dati seguenti: a) indirizzi IP; b) indirizzi URL; c) domini; d) hash dei file; e) dati del malware (nome del malware, nomi dei file e loro ubicazione, chiavi di registro specifiche associate all'attività di malware); f) dati relativi alle attività di rete (porte, protocolli, indirizzi, referrer, programmi utente, header, log specifici o schemi distintivi nel traffico di rete); g) dati del messaggio di posta elettronica (mittente, destinatario, oggetto, intestazione, contenuto); h) richieste DNS e configurazioni dei registri; i) attività dell'account utente (login, attività di account utente privilegiato, privilege escalation); j) traffico delle banche dati (lettura/scrittura), richieste relative allo stesso file. Questo tipo di informazioni può includere dati relativi, tra l'altro, agli indicatori che descrivono gli schemi nel traffico di rete corrispondenti ad attacchi noti/comunicazioni botnet, indirizzi IP delle macchine infette da malware (bot), dati relativi ai server di «comando e controllo» utilizzati dai malware (solitamente domini o indirizzi IP) e URL relativi a siti di phishing o a siti web osservati che ospitano malware o sfruttano kit.	Sì, se sono disponibili informazioni sugli indicatori di compromissione connessi alla minaccia informatica.	Alfanumerico
20.	Altre informazioni pertinenti	Qualsiasi altra informazione pertinente sulla minaccia informatica significativa.	Sì, se del caso e se sono disponibili altre informazioni non contemplate nel modello.	Alfanumerico