Consiglio
dell'Unione europea

Bruxelles, 15 marzo 2024
(OR. en)

7871/24

EF 112
ECOFIN 329
CYBER 91
TELECOM 122
DELACT 79

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	13 marzo 2024
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	C(2024) 1519 final
Oggetto:	REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE del 13.3.2024 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

Si trasmette in allegato, per le delegazioni, il documento C(2024) 1519 final.

All.: C(2024) 1519 final

COMMISSIONE
EUROPEA

Bruxelles, 13.3.2024
C(2024) 1519 final

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 13.3.2024

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

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELL'ATTO DELEGATO

Uno degli obiettivi del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (DORA) è quello di armonizzare e razionalizzare il regime di segnalazione degli incidenti connessi alle TIC per le entità finanziarie nell'UE. A tal fine il DORA introduce requisiti coerenti per le entità finanziarie in materia di gestione, classificazione e segnalazione degli incidenti connessi alle TIC.

A tale riguardo, l'articolo 18, paragrafo 3, del DORA dà mandato alle autorità europee di vigilanza (AEV) di elaborare, tramite il comitato congiunto e in consultazione con la BCE e l'ENISA, progetti di norme tecniche di regolamentazione comuni che specifichino ulteriormente gli aspetti seguenti:

(a) i criteri per la classificazione e la determinazione dell'impatto degli incidenti connessi alle TIC di cui all'articolo 18, paragrafo 1, del DORA, comprese le soglie di rilevanza per la determinazione dei gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o di sicurezza dei pagamenti, che sono oggetto dell'obbligo di segnalazione di cui all'articolo 19, paragrafo 1, del DORA;

(b) i criteri che le autorità competenti devono applicare per valutare la pertinenza dei gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o di sicurezza dei pagamenti rispetto alle autorità competenti interessate in altri Stati membri, nonché i dettagli delle segnalazioni di gravi indicenti TIC o, ove applicabile, di gravi incidenti operativi o di sicurezza dei pagamenti da condividere con altre autorità competenti ai sensi dell'articolo 19, paragrafi 6 e 7, del DORA; nonché

(c) i criteri per classificare le minacce informatiche come significative, comprese soglie di rilevanza elevate per la determinazione delle minacce informatiche significative.

Il presente regolamento delegato corrisponde a tale mandato ed è stato trasmesso alla Commissione il 17 gennaio 2024.

L'ENISA e la BCE hanno partecipato al sottocomitato del comitato congiunto delle AEV sulla resilienza operativa digitale (JC SC DOR).

2. CONSULTAZIONI PRECEDENTI L'ADOZIONE DELL'ATTO

Nell'ambito dell'elaborazione delle norme di cui al presente progetto di regolamento, il 19 giugno 2023 le autorità europee di vigilanza hanno pubblicato il progetto di norme tecniche di regolamentazione per una consultazione di tre mesi, che si è conclusa l'11 settembre 2023. Sono pervenute alle AEV 105 risposte da parte di una varietà di partecipanti al mercato del settore finanziario. La relazione finale delle AEV fornisce una panoramica completa delle risposte dei portatori di interessi[1].

I partecipanti alla consultazione pubblica si sono espressi su tutti gli aspetti del progetto di norme tecniche di regolamentazione proposto. I punti principali sollevati sono stati i seguenti:

- **l'approccio per la classificazione degli incidenti gravi**: secondo molti partecipanti alla consultazione pubblica l'approccio di classificazione è eccessivamente

[1] Autorità europee di vigilanza (2024), "Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554".

complesso e il processo di segnalazione crea difficoltà alle entità finanziarie durante la gestione degli incidenti. Alcuni di tali partecipanti hanno anche proposto di modificare la ponderazione dei diversi criteri per adattarli meglio al rispettivo settore (ad esempio lo spostamento del criterio "Clienti, controparti finanziarie e transazioni interessati" tra quelli secondari, l'innalzamento del criterio "Durata e periodo di inattività del servizio" a criterio primario ecc.). Diversi partecipanti hanno inoltre proposto che l'approccio alla classificazione previsto dalle norme tecniche di regolamentazione si concentri più direttamente sull'impatto dell'incidente;

- **i criteri di classificazione e le relative soglie di rilevanza**: i criteri di classificazione definiti nelle norme tecniche di regolamentazione riguardano "Clienti, controparti finanziarie e transazioni interessati", "Impatto reputazionale", "Durata e periodo di inattività del servizio", "Estensione geografica", "Perdite di dati", "Servizi critici colpiti" e "Impatto economico". I portatori di interessi hanno generalmente auspicato ulteriori chiarimenti (ad esempio su come calcolare le soglie) e spesso hanno chiesto di innalzare le soglie di rilevanza;
- **gli incidenti ricorrenti**: numerosi partecipanti hanno espresso preoccupazioni per l'onere operativo, compresi l'impiego sostanziale di risorse interne e la difficoltà di valutare i dati, che deriverebbe dall'analisi degli incidenti finalizzata a individuare le analogie. Alcuni di loro hanno anche espresso preoccupazioni sulla proporzionalità, in quanto tale requisito inciderebbe in modo sproporzionato sulle entità di dimensioni minori;
- **la proporzionalità**: i portatori di interessi hanno sottolineato anche l'importanza di garantire la proporzionalità. Inoltre il comitato consultivo congiunto delle AEV sulla proporzionalità ha fornito una consulenza ad hoc su come rafforzare la proporzionalità del progetto di norme tecniche di regolamentazione.

Alla luce delle osservazioni ricevute, le AEV hanno apportato modifiche al progetto di norme tecniche di regolamentazione. Tali modifiche riguardano l'approccio alla classificazione, la specificazione di alcuni criteri di classificazione e delle relative soglie di rilevanza nonché l'approccio agli incidenti ricorrenti:

- per quanto riguarda l'approccio alla classificazione, le AEV hanno modificato il progetto di norme tecniche di regolamentazione in modo che le entità finanziarie classifichino gli incidenti come gravi se è soddisfatto il criterio "Servizi critici colpiti" e se i) è individuato un accesso doloso non autorizzato ai sistemi informatici e di rete nell'ambito del criterio "Perdite di dati" o ii) sono raggiunte le soglie di rilevanza di altri due criteri;
- per quanto riguarda i criteri di classificazione e le relative soglie, pur mantenendo un approccio armonizzato per la classificazione degli incidenti per tutte le AEV che rientrano nell'ambito di applicazione del DORA, le AEV hanno chiarito i vari aspetti della classificazione nei criteri e hanno introdotto modifiche alle soglie dei criteri "Clienti, controparti finanziarie e transazioni interessati" e "Perdite di dati" al fine di introdurre una maggiore proporzionalità, affrontare le questioni specifiche del settore sollevate e rilevare gli incidenti informatici pertinenti;
- infine, per rispondere alle preoccupazioni sull'onere di segnalazione per le entità finanziarie, le AEV hanno modificato l'approccio per la classificazione degli incidenti ricorrenti, che ora si concentra sugli incidenti che si sono verificati almeno due volte, che hanno la stessa apparente causa di fondo e che avrebbero soddisfatto

cumulativamente i criteri di classificazione degli incidenti. La valutazione della ricorrenza deve essere effettuata su base mensile.

3. ELEMENTI GIURIDICI DELL'ATTO DELEGATO

Il capo I stabilisce i criteri di classificazione degli incidenti in base a clienti, controparti finanziarie e transazioni (articolo 1), impatto reputazionale (articolo 2), durata e periodo di inattività del servizio (articolo 3), estensione geografica (articolo 4), perdite di dati (articolo 5), criticità dei servizi interessati (articolo 6) e impatto economico (articolo 7).

Il capo II stabilisce le condizioni per classificare un incidente come grave e le modalità di gestione degli incidenti ricorrenti (articolo 8) e le relative soglie di rilevanza (articolo 9).

Il capo III riguarda le minacce informatiche significative e stabilisce le soglie di rilevanza per determinare quando una minaccia informatica è significativa (articolo 10).

Il capo IV stabilisce le norme per determinare se un incidente grave è pertinente rispetto alle autorità competenti di altri Stati membri (articolo 11) e le modalità di condivisione dei dettagli relativi agli incidenti gravi con altre autorità competenti (articolo 12).

Il capo V contiene le disposizioni finali sull'entrata in vigore (articolo 13).

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 13.3.2024

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

(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[2], in particolare l'articolo 18, paragrafo 4, terzo comma,

considerando quanto segue:

(1) Il regolamento (UE) 2022/2554 mira ad armonizzare e razionalizzare gli obblighi di segnalazione degli incidenti connessi alle TIC e degli incidenti operativi o relativi alla sicurezza dei pagamenti riguardanti enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica ("incidenti"). Dato che gli obblighi di segnalazione riguardano 20 tipi diversi di entità finanziarie, i criteri di classificazione e le soglie di rilevanza per determinare gli incidenti gravi e le minacce informatiche significative dovrebbero essere specificati in modo semplice, armonizzato e coerente, tenendo conto delle specificità dei servizi e delle attività di tutte le entità finanziarie interessate.

(2) Al fine di garantire la proporzionalità, i criteri di classificazione e le soglie di rilevanza dovrebbero riflettere le dimensioni e il profilo di rischio complessivo nonché la natura, la portata e la complessità dei servizi di tutte le entità finanziarie. Inoltre i criteri e le soglie di rilevanza dovrebbero essere concepiti in modo tale da essere applicati in modo coerente a tutte le entità finanziarie, indipendentemente dalle loro dimensioni e dal loro profilo di rischio, e non comportare un onere di segnalazione sproporzionato per le entità finanziarie più piccole. Tuttavia, per far fronte a situazioni in cui un numero significativo di clienti è interessato da un incidente che, di per sé, non supera la soglia applicabile, è opportuno stabilire una soglia assoluta principalmente mirata alle entità finanziarie più grandi.

(3) In relazione ai quadri per la segnalazione degli incidenti, che esistevano prima dell'entrata in vigore del regolamento (UE) 2022/2554, è opportuno garantire la continuità per le entità finanziarie. I criteri di classificazione e le soglie di rilevanza

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

dovrebbero pertanto essere allineati e ispirati agli orientamenti dell'ABE sulla segnalazione degli incidenti gravi ai sensi della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio[3], agli orientamenti sulle informazioni periodiche e sulla comunicazione delle modifiche sostanziali che i repertori di dati sulle negoziazioni devono presentare all'ESMA, al quadro di riferimento della BCE/SSM per la segnalazione degli incidenti informatici e ad altri orientamenti pertinenti. I criteri di classificazione e le soglie dovrebbero inoltre essere idonei per le entità finanziarie non erano soggette agli obblighi di segnalazione degli incidenti prima del regolamento (UE) 2022/2554.

(4) Per quanto riguarda il criterio di classificazione "Quantità o numero di transazioni interessate", il concetto di transazione è ampio e riguarda differenti attività e servizi in tutti gli atti settoriali applicabili alle entità finanziarie. Ai fini di tale criterio di classificazione dovrebbero essere incluse le operazioni di pagamento e tutte le forme di scambio di strumenti finanziari, cripto-attività, merci o qualsiasi altra attività, anche sotto forma di margine, garanzia o pegno, sia a fronte di contanti che di qualsiasi altra attività. Ai fini della classificazione si dovrebbero prendere in considerazione tutte le transazioni che coinvolgono attività il cui valore può essere espresso in termini monetari.

(5) I criteri di classificazione dovrebbero garantire che siano rilevati tutti i tipi pertinenti di incidenti gravi. Molti criteri di classificazione non sono necessariamente in grado di rilevare attacchi informatici collegati all'intrusione nella rete o nei sistemi informatici. Si tratta tuttavia di elementi importanti, poiché qualsiasi intrusione nei sistemi informatici e di rete può nuocere all'entità finanziaria. Di conseguenza i criteri di classificazione "Servizi critici colpiti" e "Perdite di dati" dovrebbero essere specificati in modo tale da rilevare questi tipi di incidenti gravi, in particolare le intrusioni non autorizzate che, anche qualora gli impatti non siano immediatamente noti, possono comportare gravi conseguenze, in particolare violazioni e fughe di dati.

(6) Dato che gli enti creditizi sono soggetti sia al quadro di classificazione degli incidenti di cui all'articolo 18 del regolamento (UE) 2022/2554 sia al quadro relativo al rischio operativo di cui al regolamento delegato (UE) 2018/959 della Commissione[4], l'approccio per la valutazione dell'impatto economico di un incidente basato sul calcolo dei costi e delle perdite dovrebbe essere il più possibile coerente in entrambi i quadri normativi per evitare di introdurre requisiti incompatibili o contraddittori.

(7) Il criterio relativo all'estensione geografica di un incidente di cui all'articolo 18, paragrafo 1, lettera c), del regolamento (UE) 2022/2554 dovrebbe concentrarsi sull'impatto transfrontaliero dell'incidente, poiché l'impatto di un incidente sull'attività di un'entità finanziaria all'interno di una singola giurisdizione sarà rilevato dagli altri criteri stabiliti nel suddetto articolo.

---

[3] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

[4] Regolamento delegato (UE) 2018/959 della Commissione, del 14 marzo 2018, che integra il regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio per quanto riguarda norme tecniche di regolamentazione per la determinazione della metodologia di valutazione in virtù della quale le autorità competenti autorizzano gli enti a utilizzare metodi avanzati di misurazione per il rischio operativo (GU L 169 del 6.7.2018, pag. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(8) Dato che i criteri di classificazione sono interdipendenti e collegati tra loro, l'approccio per individuare gli incidenti gravi da segnalare ai sensi dell'articolo 19, paragrafo 1, del regolamento (UE) 2022/2554 dovrebbe basarsi su una combinazione di criteri, in cui alcuni criteri che sono strettamente correlati alle definizioni di incidente connesso alle TIC e di grave incidente TIC di cui all'articolo 3, punti 8) e 10), del regolamento (UE) 2022/2554 dovrebbero avere maggiore importanza nella classificazione degli incidenti gravi rispetto ad altri criteri.

(9) Per garantire che le segnalazioni e le notifiche di incidenti gravi ricevute dalle autorità competenti ai sensi dell'articolo 19, paragrafo 1, del regolamento (UE) 2022/2554 servano sia a fini di vigilanza che di prevenzione del contagio nel settore finanziario, le soglie di rilevanza dovrebbero consentire di rilevare gli incidenti gravi, concentrandosi, tra l'altro, sull'impatto sui servizi critici specifici dell'entità, sulle soglie specifiche assolute e relative di clienti o controparti finanziarie, sulle transazioni che indicano un impatto significativo sull'entità finanziaria e sulla rilevanza dell'impatto in altri Stati membri.

(10) Gli incidenti che interessano i servizi TIC o i sistemi informatici e di rete a supporto di funzioni essenziali o importanti o che interessano i servizi finanziari che richiedono un'autorizzazione, oppure l'accesso doloso non autorizzato a sistemi informatici e di rete a supporto di funzioni essenziali o importanti dovrebbero essere considerati incidenti che interessano i servizi essenziali delle entità finanziarie. L'accesso doloso e non autorizzato ai sistemi informatici e di rete a supporto di funzioni essenziali o importanti delle entità finanziarie comporta seri rischi per l'entità finanziaria e, poiché potrebbe avere ripercussioni su altre entità finanziarie, dovrebbe sempre essere considerato un incidente grave da segnalare.

(11) Gli incidenti ricorrenti collegati da un'apparente causa di fondo simile, che singolarmente non costituiscono un incidente grave, possono indicare carenze e punti deboli significativi nelle procedure di gestione degli incidenti e dei rischi dell'entità finanziaria. È pertanto opportuno che gli incidenti ricorrenti siano considerati collettivamente incidenti gravi quando si verificano ripetutamente per un determinato periodo di tempo.

(12) Dal momento che le minacce informatiche possono avere un impatto negativo sull'entità e sul settore finanziario, le minacce informatiche significative che le entità finanziarie possono comunicare dovrebbero indicare la probabilità di concretizzazione e la criticità dell'impatto potenziale. Di conseguenza, per garantire una valutazione chiara e coerente della rilevanza delle minacce informatiche, la classificazione di una minaccia informatica come significativa dovrebbe dipendere dalla probabilità che i criteri di classificazione per gli incidenti gravi e la relativa soglia sarebbero soddisfatti laddove la minaccia si concretizzasse, nonché dal tipo di minaccia informatica e dalle informazioni a disposizione dell'entità finanziaria.

(13) Tenuto conto che gli incidenti che hanno un impatto su entità finanziarie e clienti nella giurisdizione di altri Stati membri devono essere notificati alle autorità competenti di questi ultimi, la valutazione dell'impatto in un'altra giurisdizione ai sensi dell'articolo 19, paragrafo 7, del regolamento (UE) 2022/2554 dovrebbe basarsi sulla causa di fondo dell'incidente, sul potenziale contagio attraverso fornitori terzi e alle infrastrutture dei mercati finanziari, nonché sull'impatto dell'incidente su gruppi significativi di clienti o controparti finanziarie.

(14) I processi di segnalazione e notifica di cui all'articolo 19, paragrafi 6 e 7, del regolamento (UE) 2022/2554 dovrebbero consentire ai rispettivi destinatari di valutare

l'impatto degli incidenti. Le informazioni trasmesse dovrebbero pertanto includere tutti i dettagli contenuti nelle segnalazioni degli incidenti presentate dall'entità finanziaria all'autorità competente.

(15) Qualora un incidente costituisca una violazione di dati personali ai sensi del regolamento (UE) 2016/679 e della direttiva 2002/58/CE, il presente regolamento non dovrebbe incidere sugli obblighi di registrazione e notifica delle violazioni dei dati personali previsti da tali normative dell'Unione. Le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE.

(16) Il presente regolamento si basa sul progetto di norme tecniche di regolamentazione presentato alla Commissione dalle autorità europee di vigilanza, in consultazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e la Banca centrale europea (BCE).

(17) Il comitato congiunto delle autorità europee di vigilanza di cui all'articolo 54 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio[5], all'articolo 54 del regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio[6] e all'articolo 54 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio[7] ha condotto consultazioni pubbliche sul progetto di norme tecniche di regolamentazione su cui si basa il presente regolamento, ha analizzato i potenziali costi e benefici delle norme proposte e ha chiesto il parere del gruppo delle parti interessate nel settore bancario, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1093/2010, dei gruppi delle parti interessate nel settore dell'assicurazione e della riassicurazione e nel settore dei fondi pensionistici aziendali e professionali, istituiti ai sensi dell'articolo 37 del regolamento (UE) n. 1094/2010, e del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1095/2010.

(18) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[8], il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 24 gennaio 2024,

---

5 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).

6 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).

7 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).

8 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).

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I
Criteri di classificazione

Articolo 1
Clienti, controparti finanziarie e transazioni

1. Il numero di clienti interessati dall'incidente, di cui all'articolo 18, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, riflette il numero di tutti i clienti interessati, siano essi persone fisiche o giuridiche, che sono o sono stati impossibilitati a usufruire del servizio fornito dall'entità finanziaria durante l'incidente o che hanno subito un impatto negativo a causa dell'incidente. Tale numero comprende anche i terzi esplicitamente coperti dall'accordo contrattuale tra l'entità finanziaria e il cliente come beneficiari del servizio interessato.

2. Il numero di controparti finanziarie interessate dall'incidente, di cui all'articolo 18, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, riflette il numero di tutte le controparti finanziarie interessate che hanno concluso un accordo contrattuale con l'entità finanziaria.

3. Per quanto riguarda la rilevanza dei clienti e delle controparti finanziarie interessati dall'incidente, di cui all'articolo 18, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, l'entità finanziaria tiene conto della misura in cui l'impatto su un cliente o una controparte finanziaria inciderà sulla realizzazione degli obiettivi commerciali dell'entità finanziaria nonché del potenziale impatto dell'incidente sull'efficienza del mercato.

4. Per quanto riguarda la quantità o il numero di transazioni interessate dall'incidente, di cui all'articolo 18, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, l'entità finanziaria tiene conto di tutte le transazioni interessate che implichino un importo monetario quando almeno una parte della transazione è effettuata nell'Unione.

5. Qualora non sia possibile determinare il numero effettivo di clienti o di controparti finanziarie interessati o la quantità o il numero effettivo di transazioni interessate, l'entità finanziaria stima tali numeri o quantità sulla base dei dati disponibili relativi a periodi di riferimento comparabili.

Articolo 2
Impatto reputazionale

1. Ai fini della determinazione dell'impatto reputazionale dell'incidente, di cui all'articolo 18, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, le entità finanziarie ritengono che si sia verificato un impatto reputazionale se è soddisfatto almeno uno dei criteri seguenti:

   (a) l'incidente è stato riportato dai media;

   (b) l'incidente 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;

   (c) a seguito dell'incidente l'entità finanziaria non sarà in grado o potrebbe non essere in grado di soddisfare i requisiti normativi;

(d) a seguito dell'incidente l'entità finanziaria perderà o potrebbe perdere clienti o controparti finanziarie, con un impatto significativo sulla sua attività.

2. Nel valutare l'impatto reputazionale dell'incidente le entità finanziarie tengono conto del livello di visibilità che l'incidente ha acquisito o potrebbe acquisire in relazione a ciascun criterio di cui al paragrafo 1.

Articolo 3
Durata e periodo di inattività del servizio

1. Le entità finanziarie misurano la durata di un incidente, di cui all'articolo 18, paragrafo 1, lettera b), del regolamento (UE) 2022/2554, dal momento in cui si verifica l'incidente fino al momento in cui è risolto.

Qualora non siano in grado di determinare il momento in cui si è verificato l'incidente, le entità finanziarie misurano la durata dell'incidente a partire dal momento in cui è stato individuato. Qualora vengano a conoscenza del fatto che l'incidente si è verificato prima della sua individuazione, le entità finanziarie misurano la durata a partire dal momento in cui l'incidente è stato registrato nei registri di rete o di sistema o in altre fonti di dati.

Qualora non sappiano ancora quando l'incidente sarà risolto o non siano in grado di verificare le registrazioni nei registri o in altre fonti di dati, le entità finanziarie applicano stime.

2. Le entità finanziarie misurano il periodo di inattività del servizio di un incidente, di cui all'articolo 18, paragrafo 1, lettera b), del regolamento (UE) 2022/2554, 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. Se il periodo di inattività del servizio causa un ritardo nella fornitura del servizio dopo che sono state ripristinate le regolari attività o operazioni, il periodo di inattività è misurato dall'inizio dell'incidente fino al momento della fornitura integrale del servizio che ha subito il ritardo.

Qualora non siano in grado di determinare il momento in cui è iniziato il periodo di inattività del servizio, le entità finanziarie misurano tale periodo a partire dal momento in cui è stato individuato.

Articolo 4
Estensione geografica

Ai fini della determinazione dell'estensione geografica dell'incidente, con riferimento alle aree colpite, di cui all'articolo 18, paragrafo 1, lettera c), del regolamento (UE) 2022/2554, le entità finanziarie valutano se l'incidente ha o ha avuto un impatto in altri Stati membri e, in particolare, la rilevanza dell'impatto in relazione a ciascuno dei seguenti soggetti:

(a) clienti e controparti finanziarie di altri Stati membri;

(b) succursali o altre entità finanziarie del gruppo che svolgono attività in altri Stati membri;

(c) infrastrutture dei mercati finanziari o fornitori terzi che potrebbero avere un impatto su entità finanziarie di altri Stati membri a cui forniscono servizi, nella misura in cui tali informazioni sono disponibili.

Articolo 5
Perdite di dati

Ai fini della determinazione delle perdite di dati derivanti dall'incidente, di cui all'articolo 18, paragrafo 1, lettera d), del regolamento (UE) 2022/2554, le entità finanziarie tengono conto di quanto segue:

(a) in relazione alla disponibilità dei dati, se l'incidente ha reso temporaneamente o permanentemente inaccessibili o inutilizzabili i dati su richiesta dell'entità finanziaria, dei suoi clienti o delle sue controparti;

(b) in relazione all'autenticità dei dati, se l'incidente ha compromesso l'affidabilità della fonte dei dati;

(c) in relazione all'integrità dei dati, se l'incidente ha comportato una modifica non autorizzata dei dati che li ha resi inesatti o incompleti;

(d) in relazione alla riservatezza dei dati, se l'incidente ha comportato l'accesso ai dati da parte di un soggetto o sistema non autorizzato o la loro divulgazione a tale soggetto o sistema.

Articolo 6
Criticità dei servizi colpiti

Ai fini della determinazione della criticità dei servizi colpiti di cui all'articolo 18, paragrafo 1, lettera e), del regolamento (UE) 2022/2554, le entità finanziarie valutano se l'incidente:

(a) interessa o ha interessato servizi TIC o sistemi informatici e di rete a supporto di funzioni essenziali o importanti dell'entità finanziaria;

(b) interessa o ha interessato servizi finanziari forniti dall'entità finanziaria che richiedono l'autorizzazione, la registrazione o che sono sottoposti a vigilanza da parte delle autorità competenti;

(c) costituisce o ha costituito un accesso non autorizzato, doloso e riuscito ai sistemi informatici e di rete dell'entità finanziaria.

Articolo 7
Impatto economico

1. Ai fini della determinazione dell'impatto economico dell'incidente, di cui all'articolo 18, paragrafo 1, lettera f), del regolamento (UE) 2022/2554, le entità finanziarie prendono in considerazione, senza tener conto dei recuperi finanziari, i tipi di costi e perdite diretti e indiretti di seguito elencati, sostenuti a seguito dell'incidente:

   (a) fondi o attività finanziarie espropriati di cui sono responsabili, comprese le attività perdute per furto;

   (b) costi per la sostituzione o il trasferimento di software, hardware o infrastrutture;

   (c) 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) spese dovute all'inosservanza degli obblighi contrattuali;

(e) costi di risarcimenti e indennizzi ai clienti;

(f) perdite dovute a mancati introiti;

(g) costi associati alla comunicazione interna ed esterna;

(h) costi di consulenza, compresi i costi associati alla consulenza legale, ai servizi forensi e ai servizi per rimediare all'incidente.

2. I costi e le perdite di cui al paragrafo 1 non comprendono i costi necessari per il funzionamento quotidiano dell'attività, in particolare:

(a) i costi per la manutenzione generale di infrastrutture, attrezzature, hardware e software e i costi per l'aggiornamento delle competenze del personale;

(b) i costi interni o esterni per migliorare l'attività dopo l'incidente, compresi aggiornamenti, miglioramenti e iniziative di valutazione del rischio;

(c) i premi assicurativi.

3. Le entità finanziarie calcolano gli importi dei costi e delle perdite sulla base dei dati disponibili al momento della segnalazione. Qualora non sia possibile determinare gli importi effettivi dei costi e delle perdite, le entità finanziarie effettuano una stima di tali importi.

4. Nel valutare l'impatto economico dell'incidente, le entità finanziarie sommano i costi e le perdite di cui al paragrafo 1.

Capo II
Gravi incidenti e soglie di rilevanza

Articolo 8
Gravi incidenti

1. Un incidente è considerato grave ai fini dell'articolo 19, paragrafo 1, del regolamento (UE) 2022/2554 se ha interessato i servizi critici di cui all'articolo 6 e se è soddisfatta una delle condizioni seguenti:

(a) è raggiunta la soglia di rilevanza di cui all'articolo 9, paragrafo 5, lettera b);

(b) sono raggiunte due o più delle altre soglie di rilevanza di cui all'articolo 9, paragrafi da 1 a 6.

2. Gli incidenti ricorrenti che singolarmente non sono considerati incidenti gravi ai sensi del paragrafo 1 sono considerati un unico grave incidente se soddisfano tutte le condizioni seguenti:

(a) si sono verificati almeno due volte nell'arco di sei mesi;

(b) presentano la stessa apparente causa di fondo di cui all'articolo 20, lettera b), del regolamento (UE) 2022/2554;

(c) soddisfano collettivamente i criteri per essere considerati un grave incidente di cui al paragrafo 1.

Le entità finanziarie valutano l'esistenza di incidenti ricorrenti su base mensile.

Il presente paragrafo non si applica alle microimprese e alle entità finanziarie elencate all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554.

Articolo 9

Soglie di rilevanza per la determinazione dei gravi incidenti

1. La soglia di rilevanza per il criterio "Clienti, controparti finanziarie e transazioni" è raggiunta quando una qualsiasi delle condizioni seguenti è soddisfatta:

   (a) il numero di clienti interessati è superiore al 10 % di tutti i clienti che utilizzano il servizio interessato;

   (b) il numero di clienti interessati che utilizzano il servizio interessato è superiore a 100 000;

   (c) il numero di controparti finanziarie interessate è superiore al 30 % di tutte le controparti finanziarie che svolgono attività connesse alla fornitura del servizio interessato;

   (d) il numero di transazioni interessate è superiore al 10 % del numero medio giornaliero di transazioni effettuate dall'entità finanziaria in relazione al servizio interessato;

   (e) la quantità di transazioni interessate è superiore al 10 % del valore medio giornaliero delle transazioni effettuate dall'entità finanziaria in relazione al servizio interessato;

   (f) sono stati colpiti clienti o controparti finanziarie individuati come rilevanti ai sensi dell'articolo 1, paragrafo 3.

   Qualora non sia possibile determinare il numero effettivo di clienti o di controparti finanziarie interessati o la quantità o il numero effettivo di transazioni interessate, l'entità finanziaria stima tali numeri o quantità sulla base dei dati disponibili relativi a periodi di riferimento comparabili.

2. La soglia di rilevanza per il criterio "Impatto reputazionale" è raggiunta quando è soddisfatta una qualsiasi delle condizioni di cui all'articolo 2, lettere da a) a d).

3. La soglia di rilevanza per il criterio "Durata e periodo di inattività del servizio" è raggiunta quando una qualsiasi delle condizioni seguenti è soddisfatta:

   (a) la durata dell'incidente è superiore a 24 ore;

   (b) il periodo di inattività del servizio è superiore a due ore per i servizi TIC a supporto di funzioni essenziali o importanti.

4. La soglia di rilevanza per il criterio "Estensione geografica" è raggiunta quando l'incidente ha un impatto in due o più Stati membri, in conformità dell'articolo 4.

5. La soglia di rilevanza per il criterio "Perdite di dati" è raggiunta quando una qualsiasi delle condizioni seguenti è soddisfatta:

   (a) qualsiasi impatto di cui all'articolo 5 sulla disponibilità, sull'autenticità, sull'integrità o sulla riservatezza dei dati ha o avrà un impatto negativo sulla realizzazione degli obiettivi commerciali dell'entità finanziaria o sulla sua capacità di soddisfare i requisiti normativi;

   (b) i sistemi informatici e di rete sono oggetto di accessi non autorizzati, dolosi e riusciti non contemplati alla lettera a), laddove tali accessi possono comportare perdite di dati.

6. La soglia di rilevanza per il criterio "Impatto economico" è raggiunta quando i costi e le perdite sostenuti dall'entità finanziaria a causa dell'incidente hanno superato o potrebbero superare 100 000 EUR.

Capo III
Minacce informatiche significative

Articolo 10

Soglie di rilevanza elevate per la determinazione delle minacce informatiche significative

Ai fini dell'articolo 18, paragrafo 2, del regolamento (UE) 2022/2554 una minaccia informatica è considerata significativa se sono soddisfatte tutte le condizioni seguenti:

(a) la minaccia informatica, se si concretizza, potrebbe interessare o avrebbe potuto interessare funzioni essenziali o importanti dell'entità finanziaria, o potrebbe interessare altre entità finanziarie, fornitori terzi, clienti o controparti finanziarie, sulla base delle informazioni a disposizione dell'entità finanziaria;

(b) la minaccia informatica ha un'elevata probabilità di concretizzarsi presso l'entità finanziaria o altre entità finanziarie, tenendo conto almeno degli elementi seguenti:

  i) i rischi applicabili relativi alla minaccia informatica di cui alla lettera a), comprese le potenziali vulnerabilità dei sistemi dell'entità finanziaria che possono essere sfruttate;

  ii) le capacità e le intenzioni degli attori delle minacce nella misura in cui l'entità finanziaria ne è a conoscenza;

  iii) la persistenza della minaccia e qualsiasi conoscenza acquisita sugli incidenti che hanno interessato l'entità finanziaria o i suoi fornitori terzi, clienti o controparti finanziarie;

(c) la minaccia informatica, se si concretizza, potrebbe soddisfare o raggiungere uno degli elementi seguenti:

  i) il criterio relativo alla criticità dei servizi di cui all'articolo 18, paragrafo 1, lettera e), del regolamento (UE) 2022/2554, come specificato all'articolo 6 del presente regolamento;

  ii) la soglia di rilevanza di cui all'articolo 9, paragrafo 1;

  iii) la soglia di rilevanza di cui all'articolo 9, paragrafo 4.

Qualora, a seconda del tipo di minaccia informatica e delle informazioni disponibili, l'entità finanziaria concluda che le soglie di rilevanza di cui all'articolo 9, paragrafi 2, 3, 5 e 6, potrebbero essere raggiunte, possono essere prese in considerazione anche tali soglie.

Capo IV
Pertinenza dei gravi incidenti rispetto alle autorità competenti di altri Stati membri e dettagli delle segnalazioni da condividere con altre autorità competenti

Articolo 11
Pertinenza dei gravi incidenti rispetto alle autorità competenti in altri Stati membri

La valutazione della pertinenza del grave incidente rispetto alle autorità competenti di altri Stati membri, di cui all'articolo 19, paragrafo 7, del regolamento (UE) 2022/2554 si basa sul fatto che la causa di fondo dell'incidente abbia origine in un altro Stato membro o che l'incidente abbia o abbia avuto un impatto significativo in un altro Stato membro in relazione a uno dei seguenti soggetti:

(a) clienti o controparti finanziarie;

(b) una succursale dell'entità finanziaria o un'altra entità finanziaria del gruppo;

(c) un'infrastruttura dei mercati finanziari o un fornitore terzo che potrebbe avere un impatto sulle entità finanziarie a cui fornisce servizi.

Articolo 12
Dettagli dei gravi incidenti da condividere con altre autorità competenti

I dettagli dei gravi incidenti che le autorità competenti sono tenute a trasmettere alle altre autorità competenti ai sensi dell'articolo 19, paragrafo 6, del regolamento (UE) 2022/2554 e le notifiche che l'ABE, l'ESMA o l'EIOPA e la BCE sono tenute a trasmettere alle pertinenti autorità competenti degli altri Stati membri ai sensi dell'articolo 19, paragrafo 7, del medesimo regolamento contengono lo stesso livello di informazione, senza alcuna anonimizzazione, delle notifiche e delle segnalazioni di gravi incidenti ricevute dalle entità finanziarie ai sensi dell'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554.

Capo V
Disposizioni finali

Articolo 13
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 13.3.2024

Per la Commissione
La presidente
Ursula VON DER LEYEN