I

(Risoluzioni, raccomandazioni e pareri)

RACCOMANDAZIONI

COMITATO EUROPEO PER IL RISCHIO SISTEMICO

RACCOMANDAZIONE DEL COMITATO EUROPEO PER IL RISCHIO SISTEMICO

del 2 dicembre 2021

su un quadro paneuropeo di coordinamento sistemico degli incidenti informatici per le autorità competenti

(CERS/2021/17)

(2022/C 134/01)

IL CONSIGLIO GENERALE DEL COMITATO EUROPEO PER IL RISCHIO SISTEMICO,

visto il trattato sul funzionamento dell'Unione europea,

visto l'accordo sullo Spazio economico europeo ([1]), in particolare l'allegato IX,

Visto il regolamento (UE) n. 1092/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo alla vigilanza macroprudenziale del sistema finanziario nell'Unione europea e che istituisce il Comitato europeo per il rischio sistemico ([2]) e in particolare l'articolo 3, paragrafo 2, lettere b) e d), e gli articoli 16 e 18,

vista la decisione CERS/2011/1 del Comitato europeo per il rischio sistemico, del 20 gennaio 2011, che adotta il regolamento interno del Comitato europeo per il rischio sistemico ([3]), e in particolare gli articoli 18 e 20,

considerando quanto segue:

(1) Come indicato al considerando 4 della raccomandazione CERS/2013/1 del Comitato europeo per il rischio sistemico ([4]), l'obiettivo ultimo della politica macroprudenziale è contribuire a salvaguardare la stabilità del sistema finanziario nel suo insieme, anche attraverso il rafforzamento della capacità di tenuta del sistema finanziario e la riduzione dell'accumulo di rischi sistemici, garantendo così un apporto sostenibile del settore finanziario alla crescita economica. Il Comitato europeo per il rischio sistemico (CERS), è responsabile della vigilanza macroprudenziale del sistema finanziario all'interno dell'Unione. Nell'assolvere il proprio mandato, il CERS dovrebbe contribuire alla prevenzione e all'attenuazione dei rischi sistemici per la stabilità finanziaria, compresi quelli relativi agli incidenti informatici, e proporre le modalità per attenuare tali rischi.

(2) Gli incidenti informatici gravi possono rappresentare un rischio sistemico per il sistema finanziario, data la loro capacità di perturbare le operazioni e i servizi finanziari critici. L'amplificazione di uno shock iniziale può avvenire attraverso un contagio operativo o finanziario oppure attraverso un'erosione della fiducia nel sistema finanziario. Se il sistema finanziario non è in grado di assorbire questi shock, la stabilità finanziaria sarà a rischio e questa situazione può determinare una crisi informatica sistemica ([5]).

([1]) GU L 1, del 3.1.1994, pag. 3.
([2]) GU L 331, del 15.12.2010, pag. 1.
([3]) GU C 58 del 24.2.2011, pag. 4.
([4]) Raccomandazione CERS/2013/1 del Comitato europeo per il rischio sistemico, del 4 aprile 2013, sugli obiettivi intermedi e gli strumenti di politica macroprudenziale (GU C 170 del 15.6.2013, pag. 1).
([5]) Cfr. Systemic cyber risk, ESRB, febbraio 2020, disponibile sul sito web del CERS all'indirizzo www.esrb.europa.eu

(3) Il panorama delle minacce informatiche in continua evoluzione e il recente aumento dei principali incidenti informatici sono indicatori del maggiore rischio per la stabilità finanziaria nell'Unione. La pandemia di COVID-19 ha evidenziato l'importanza del ruolo svolto dalla tecnologia nel consentire il funzionamento del sistema finanziario. Le autorità e le istituzioni competenti hanno dovuto adeguare le proprie infrastrutture tecniche e i propri sistemi di gestione dei rischi a un improvviso aumento del lavoro a distanza, che ha aumentato l'esposizione complessiva del sistema finanziario alle minacce informatiche e ha consentito ai criminali di elaborare nuovi modi operativi e di adattare quelli esistenti al fine di sfruttare la situazione ([6]). In tale contesto, il numero di incidenti informatici segnalati alla vigilanza bancaria della BCE nel 2020 è aumentato del 54 % rispetto al 2019 ([7]).

(4) La scala, la velocità e il tasso di propagazione potenzialmente di ampie dimensioni di un grave incidente richiedono una risposta efficace da parte delle autorità competenti per attenuare i potenziali effetti negativi sulla stabilità finanziaria. Un coordinamento e una comunicazione rapidi tra le autorità competenti a livello dell'Unione possono contribuire a una valutazione precoce dell'impatto di un incidente informatico grave sulla stabilità finanziaria, mantenendo la fiducia nel sistema finanziario e limitando il contagio ad altre istituzioni finanziarie, contribuendo in tal modo a evitare che un incidente informatico grave diventi un rischio per la stabilità finanziaria.

(5) Lo shock sottostante ha origine in un modo innovativo rispetto alle tradizionali crisi finanziarie e di liquidità solitamente affrontate dalle autorità competenti. Oltre agli aspetti finanziari, la valutazione complessiva del rischio deve includere la portata e l'impatto di disfunzioni operative, in quanto queste potrebbero influenzare la scelta degli strumenti macroprudenziali. Analogamente, la stabilità finanziaria potrebbe anche influenzare la scelta dei metodi operativi di mitigazione da parte di esperti informatici. Ciò richiede uno stretto e rapido coordinamento e una comunicazione aperta al fine, tra l'altro, di sviluppare una consapevolezza della situazione.

(6) Il rischio di un mancato coordinamento da parte delle autorità esiste e deve essere affrontato. Le autorità competenti dell'Unione dovranno coordinarsi tra loro e con altre autorità, quali l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (European Union Agency for Network and Information Security, ENISA), con le quali potrebbero non interagire di solito. Poiché un numero significativo di istituzioni finanziarie dell'Unione opera a livello mondiale, è probabile che un incidente informatico grave non sia limitato all'Unione o possa essere innescato al di fuori dell'Unione e potrebbe richiedere un coordinamento globale della risposta.

(7) Le autorità competenti devono essere preparate a tali interazioni. Altrimenti rischierebbero di intraprendere azioni incoerenti che contraddicono o compromettono le risposte di altre autorità. Tale mancanza di coordinamento potrebbe amplificare lo shock per il sistema finanziario determinando un'erosione della fiducia nel funzionamento del sistema finanziario che, nel peggiore dei casi, comporterebbe un rischio per la stabilità finanziaria ([8]). Pertanto, dovrebbero essere adottate le misure necessarie per affrontare il rischio per la stabilità finanziaria derivante da un mancato coordinamento nel caso di un incidente informatico grave.

(8) La relazione del CERS (2021) «*Mitigating systemic cyber risk*» ([9]) individua la necessità di istituire un quadro paneuropeo di coordinamento sistemico degli incidenti informatici (EU-SCICF) per le autorità competenti nell'Unione. L'obiettivo dell'EU-SCICF sarebbe di aumentare il livello di preparazione delle autorità competenti per facilitare una risposta coordinata a un incidente informatico potenzialmente grave. La relazione del CERS (2021) «*Mitigating systemic cyber risk*» fornisce la valutazione del CERS sulle caratteristiche di tale quadro che sarebbero necessarie, a un primo esame, per affrontare il rischio di un mancato coordinamento.

(9) L'obiettivo principale della presente raccomandazione è portare avanti uno dei ruoli previsti delle autorità europee di vigilanza (AEV) nel quadro della proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario ([10]) (di seguito «DORA»), ossia di consentire gradualmente una risposta efficace e coordinata a livello dell'Unione in caso di un grave incidente transfrontaliero connesso alle tecnologie dell'informazione e della comunicazione (TIC) o di una minaccia connessa che abbia un impatto sistemico sul settore finanziario dell'Unione nel suo complesso. Questo processo porterà alla creazione dell'EU-SCICF per le autorità competenti.

([6]) Cfr. la valutazione della minaccia della criminalità organizzata su Internet (Internet Organised Crime Threat Assessment), Europol, 2020, disponibile sul sito web di Europol all'indirizzo www.europol.europa.eu

([7]) Cfr. IT and cyber risk: a constant challenge, BCE, 2021, disponibile sul sito Internet della vigilanza bancaria della BCE all'indirizzo www.bankingsupervision.europa.eu

([8]) Cfr. Systemic cyber risk, CERS, febbraio 2020, disponibile sul sito web del CERS all'indirizzo www.esrb.europa.eu

([9]) Cfr. Mitigating systemic cyber risk, CERS, 2021, (imminente).

([10]) COM/2020/595 final.

(10) L'EU-SCICF non dovrebbe mirare a sostituire i quadri di riferimento esistenti, ma a colmare eventuali lacune in materia di coordinamento e comunicazione tra le autorità competenti stesse e con altre autorità dell'Unione e altri attori chiave a livello internazionale. A tale riguardo, si dovrebbe considerare il posizionamento dell'EU-SCICF nell'attuale quadro di crisi finanziaria e nel panorama del quadro dell'Unione in materia di incidenti informatici. Per quanto riguarda il coordinamento tra le autorità competenti stesse, si dovrebbero tenere in considerazione, tra l'altro, i ruoli e le attività del gruppo di cooperazione in materia di reti e sistemi informativi (NIS) per i soggetti finanziari di cui alla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([11]), nonché i meccanismi di coordinamento previsti mediante l'istituzione dell'unità congiunta per il ciberspazio, unitamente al coinvolgimento dell'ENISA.

(11) In particolare, la proposta di avviare la preparazione dell'EU-SCICF mira a promuovere i potenziali ruoli delle AEV, come previsto dalla proposta di regolamento DORA. La proposta di regolamento DORA propone che «le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, la BCE e il CERS, possono istituire meccanismi che consentano la condivisione di pratiche efficaci tra i vari settori finanziari per migliorare la consapevolezza situazionale e identificare i rischi e le vulnerabilità informatiche comuni a tutti i settori» e «possono elaborare esercitazioni di gestione delle crisi e delle emergenze comprendenti scenari di attacchi informatici al fine di sviluppare canali di comunicazione e promuovere gradualmente una risposta efficace coordinata a livello dell'UE nel caso di grave incidente transfrontaliero connesso alle TIC o relativa minaccia aventi un impatto sistemico sull'intero settore finanziario dell'Unione» ([12]). Un quadro paneuropeo come l'EU-SCICF non esiste ancora e dovrebbe essere istituito e sviluppato nel contesto della DORA.

(12) Dato il rischio per la stabilità finanziaria nell'Unione derivante dal rischio informatico, i lavori preparatori per la graduale istituzione dell'UE-SCICF dovrebbero, per quanto possibile, iniziare anche prima che il quadro giuridico e politico richiesto per la sua istituzione sia pienamente applicabile. Tale quadro giuridico e politico sarebbe interamente completato e finalizzato una volta che le pertinenti disposizioni del regolamento DORA e dei relativi atti delegati diventeranno applicabili.

(13) Una comunicazione efficace contribuisce alla consapevolezza della situazione tra le autorità competenti ed è pertanto un prerequisito indispensabile per il coordinamento a livello dell'Unione in caso di incidenti informatici gravi. A tale riguardo, è opportuno definire l'infrastruttura di comunicazione necessaria per coordinare la risposta a un incidente informatico grave. Ciò richiederebbe di specificare il tipo di informazioni che devono essere condivise, i canali regolari da utilizzare per condividere tali informazioni e i punti di contatto con cui le informazioni dovrebbero essere condivise. La condivisione delle informazioni deve rispettare i requisiti giuridici vigenti. Inoltre, potrebbe essere necessario che le autorità competenti definiscano un piano d'azione chiaro e i protocolli da seguire al fine di garantire un adeguato coordinamento tra le autorità coinvolte nella pianificazione di una risposta coordinata a un incidente informatico grave.

(14) Una crisi informatica sistemica richiederà l'avvio di una piena cooperazione a livello nazionale e dell'Unione. Pertanto, la designazione di punti di contatto per le AEV, la BCE e ciascuno Stato membro tra le rispettive autorità nazionali competenti, che dovrebbero essere comunicati alle AEV, può essere prevista per stabilire i principali interlocutori nel sistema di coordinamento dell'EU-SCICF da informare in caso di incidente informatico grave. La necessità di designare punti di contatto dovrebbe essere valutata durante lo sviluppo dell'EU-SCICF, tenendo conto del punto di contatto unico designato ai sensi della direttiva (UE) 2016/1148 che gli Stati membri hanno istituito in materia di sicurezza delle reti e dei sistemi informativi per garantire la cooperazione transfrontaliera con gli altri Stati membri e con il gruppo di cooperazione NIS ([13]).

(15) Lo svolgimento di esercitazioni di gestione delle crisi e delle emergenze potrebbe facilitare l'attuazione dell'EU-SCICF e consentire alle autorità di valutare la propria prontezza e preparazione per una crisi informatica sistemica a livello dell'Unione. Tali esercitazioni fornirebbero degli insegnamenti alle autorità e consentirebbero un miglioramento e un'evoluzione continui dell'EU-SCICF.

([11]) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).
([12]) Cfr. progetto di articolo 43 della proposta di regolamento DORA.
([13]) Cfr. Commissione europea, NIS Cooperation Group, disponibile sul sito web della Commissione europea all'indirizzo ec.europa.eu

(16) Per lo sviluppo dell'EU-SCICF è essenziale che le AEV svolgano congiuntamente il lavoro preparatorio rilevante al fine di prendere in considerazione i potenziali elementi chiave del quadro di riferimento, le risorse richieste e le necessità per procedere con il suo sviluppo. In seguito, le AEV potrebbero iniziare a lavorare a un'analisi preliminare di eventuali ostacoli che potrebbero compromettere la capacità delle AEV e delle autorità competenti di istituire l'EU-SCICF e di condividere le informazioni pertinenti attraverso i canali di comunicazione in caso di incidente informatico grave. Tale analisi costituirebbe un passo importante a sostegno di qualsiasi ulteriore azione, sia di natura legislativa che di altra tipologia di sostegno, che la Commissione europea potrebbe intraprendere nella fase di attuazione post-DORA,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

SEZIONE 1

RACCOMANDAZIONI

Raccomandazione A — Istituzione di un quadro paneuropeo di coordinamento sistemico degli incidenti informatici (EU-SCICF)

1. Si raccomanda che, come previsto nella proposta della Commissione di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario (di seguito «DORA»), le autorità europee di vigilanza (AEV), congiuntamente attraverso il Comitato congiunto. e insieme alla Banca centrale europea (BCE), al Comitato europeo per il rischio sistemico (CERS) e alle autorità nazionali competenti, inizino a prepararsi allo sviluppo graduale di una risposta coordinata efficace a livello dell'Unione in caso di un grave incidente informatico transfrontaliero o di una minaccia connessa che potrebbe avere un impatto sistemico sul settore finanziario dell'Unione. I lavori preparatori per una risposta coordinata a livello dell'Unione dovrebbero comportare lo sviluppo graduale dell'EU-SCICF per le AEV, la BCE, il CERS e le autorità nazionali competenti. Ciò dovrebbe includere anche una valutazione del fabbisogno di risorse per l'efficace sviluppo dell'EU-SCICF.

2. Si raccomanda alle autorità europee di vigilanza, alla luce della sotto-raccomandazione A(1), in consultazione con la BCE e il CERS, di effettuare una mappatura e una successiva analisi degli impedimenti attuali, degli ostacoli giuridici e operativi di altro tipo per l'efficace sviluppo dell'EU-SCICF.

Raccomandazione B — Istituzione di punti di contatto dell'EU-SCICF

Si raccomanda che le AEV, la BCE e ciascuno Stato membro tra le proprie autorità nazionali competenti designino un punto di contatto principale che dovrebbe essere comunicato alle AEV. Tale elenco di contatti faciliterà lo sviluppo del quadro di riferimento e, una volta istituito l'EU-SCICF, i punti di contatto e il CERS dovrebbero essere informati in caso di incidente informatico grave. Si dovrebbe inoltre prevedere un coordinamento tra l'EU-SCICF e il punto di contatto unico designato a norma della direttiva (UE) 2016/1148 che gli Stati membri hanno istituito in materia di sicurezza delle reti e dei sistemi informativi per garantire la cooperazione transfrontaliera con gli altri Stati membri e con il gruppo di cooperazione in materia di reti e sistemi informativi.

Raccomandazione C — Adeguate misure a livello dell'Unione

Si raccomanda alla Commissione, sulla base dei risultati delle analisi effettuate conformemente alla raccomandazione A, di prendere in considerazione le misure appropriate necessarie per garantire un coordinamento efficace delle risposte agli incidenti informatici sistemici.

SEZIONE 2

ATTUAZIONE

1. **Definizioni**

Ai fini della presente raccomandazione si applicano le seguenti definizioni:

(a) per «informatico» si intende relativo alla, interno alla o per mezzo della infrastruttura informatica interconnessa alle interazioni tra persone, processi, dati e sistemi informativi ([14]);

([14]) Cfr. Cyber Lexicon, FSB, 12 novembre 2018, disponibile sul sito web dell'FSB all'indirizzo www.fsb.org.

(b) per «incidente informatico grave» si intende un incidente connesso alle TIC con un impatto avverso potenzialmente elevato sulla rete e sui sistemi informativi che sostengono funzioni critiche delle entità finanziarie ([15]);

(c) per «crisi informatica sistemica» si intende un incidente informatico grave che causa un livello di perturbazione del sistema finanziario dell'Unione che potrebbe comportare gravi conseguenze negative per il buon funzionamento del mercato interno e per il funzionamento dell'economia reale. Una crisi di questo tipo potrebbe derivare da un grave incidente informatico che provoca shock in una serie di canali, tra cui quelli operativi, di fiducia e finanziari;

(d) per «Autorità europee di vigilanza» o «AEV» si intendono l'Autorità europea di vigilanza (Autorità bancaria europea) istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([16]), insieme all'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali) istituita dal regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([17]) e all'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati) istituita dal regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([18]);

(e) per «Comitato congiunto» si intende il comitato congiunto delle autorità europee di vigilanza istituito dall'articolo 54 del regolamento (UE) n. 1093/2010, del regolamento (UE) n. 1094/2010 e del regolamento (UE) n. 1095/2010;

(f) per «autorità nazionale competente» si intende:

1. un'autorità competente o di vigilanza di uno Stato membro specificate negli atti dell'Unione di cui all'articolo 1, paragrafo 2, del regolamento (UE) n. 1093/2010, del regolamento (UE) n. 1094/2010 e del regolamento (UE) n. 1095/2010, e qualsiasi altra autorità nazionale competente specificata negli atti dell'Unione che conferiscono compiti alle AEV;

2. un'autorità competente di uno Stato membro designata in conformità delle seguenti disposizioni:

i. l'articolo 4 della direttiva n. 2013/36/UE del Parlamento europeo e del Consiglio ([19]), fatti salvi i compiti specifici attribuiti alla BCE dal regolamento (UE) n. 1024/2013 del Consiglio ([20]);

ii. l'articolo 22 della direttiva (UE) n. 2015/2366 del Parlamento europeo e del Consiglio ([21]);

iii. l'articolo 37 della direttiva 2009/110/CE del Parlamento europeo e del Consiglio ([22]);

iv. l'articolo 4 della direttiva (UE) n. 2019/2034 del Parlamento europeo e del Consiglio ([23]);

([15]) Cfr. punto 7) del progetto di articolo 3 della proposta di regolamento DORA.

([16]) 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).

([17]) 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).

([18]) 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).

([19]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi, che modifica la Direttiva 2002/87/CE e abroga le Direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

([20]) Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi (GU L 287 del 29.10.2013, pag. 63).

([21]) 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).

([22]) Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

([23]) Direttiva (UE) n. 2019/2034 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativa alla vigilanza prudenziale sulle imprese di investimento e recante modifica delle direttive 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE e 2014/65/UE (GU L 314 del 5.12.2019, pag. 64).

v. l'articolo 3, paragrafo 1, lettera ee), primo trattino, della proposta di regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 ([24]);

vi. l'articolo 11 del regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio ([25]);

vii. l'articolo 22 del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([26]);

viii. l'articolo 67 della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([27]);

ix. l'articolo 22 del regolamento (UE) n. 648/2012;

x. l'articolo 44 della direttiva 2011/61/UE del Parlamento europeo e del Consiglio ([28]);

xi. l'articolo 97 della direttiva 2009/65/UE del Parlamento europeo e del Consiglio ([29]);

xii. l'articolo 30 della direttiva 2009/138/CE del Parlamento europeo e del Consiglio ([30]);

xiii. l'articolo 12 della Direttiva (UE) n. 2016/97 del Parlamento europeo e del Consiglio ([31]);

xiv. l'articolo 47 della Direttiva (UE) n. 2016/2341 del Parlamento europeo e del Consiglio ([32]);

xv. l'articolo 22 del Regolamento (UE) n. 1060/2009 del Parlamento europeo e del Consiglio ([33]);

xvi. l'articolo 3, paragrafo 2 e l'articolo 32 della direttiva 2006/43/CE del Parlamento europeo e del Consiglio ([34]);

xvii. l'articolo 40 del regolamento (UE) 2016/1011 del Parlamento europeo e del Consiglio ([35]);

xviii. l'articolo 29 del regolamento (UE) 2020/1503 del Parlamento europeo e del Consiglio ([36]);

([24]) COM/2020/593 final.

([25]) Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle Direttive 98/26/CE e 2014/65/UE e del Regolamento (UE) n. 236/2012 (GU L 257 del 28.8.2014, pag. 1).

([26]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).

([27]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

([28]) Direttiva 2011/61/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n. 1060/2009 e (UE) n. 1095/2010 (GU L 174 dell'1.7.2011, pag. 1).

([29]) Direttiva 2009/65/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM) (GU L 302 del 17.11.2009, pag. 32).

([30]) Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

([31]) Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio, del 20 gennaio 2016, sulla distribuzione assicurativa (GU L 26 del 2.2.2016, pag. 19).

([32]) Direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio, del 14 dicembre 2016, relativa alle attività e alla vigilanza degli enti pensionistici aziendali o professionali (EPAP) (GU L 354 del 23.12.2016, pag. 37).

([33]) Regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito (GU L 302 del 17.11.2009, pag. 1).

([34]) Direttiva 2006/43/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio (GU L 157 del 9.6.2006, pag. 87).

([35]) Regolamento (UE) 2016/1011 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sugli indici usati come indici di riferimento negli strumenti finanziari e nei contratti finanziari o per misurare la performance di fondi di investimento e recante modifica delle direttive 2008/48/CE e 2014/17/UE e del regolamento (UE) n. 596/2014 (GU L 171 del 29.6.2016, pag.1).

([36]) Regolamento (UE) 2020/1503 del Parlamento europeo e del Consiglio, del 7 ottobre 2020, relativo ai fornitori europei di servizi di crowdfunding per le imprese, e che modifica il regolamento (UE) 2017/1129 e la direttiva (UE) 2019/1937 (GU L 347 del 20.10.2020, pag. 1).

3. un'autorità incaricata dell'adozione e/o dell'attivazione di misure di politica macroprudenziale o di altri compiti in materia di stabilità finanziaria, ad esempio un'analisi di supporto correlata, tra cui, ma non solo:

   i. un'autorità designata a norma del titolo VII, capo 4, della direttiva 2013/36/UE o dell'articolo 458, paragrafo 1, del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([37]);

   ii. un'autorità macroprudenziale con gli obiettivi, le misure, i compiti, i poteri, gli strumenti, gli obblighi di rendicontazione e le altre caratteristiche di cui alla raccomandazione CERS/2011/3 del Comitato europeo per il rischio sistemico ([38]);

(g) per «autorità competente» si intende:

1. una AEV;

2. la BCE per i compiti ad essa attribuiti ai sensi degli articoli 4, paragrafi 1 e 2, e dell'articolo 5, paragrafo 2, del regolamento (UE) n. 1024/2013;

3. un'autorità nazionale competente.

2. **Criteri di attuazione**

Ai fini dell'attuazione della presente raccomandazione si applicano i seguenti criteri:

(a) si dovrebbe prestare la debita attenzione al principio della necessità di conoscere e al principio di proporzionalità, tenendo conto degli obiettivi e dei contenuti di ciascuna raccomandazione;

(b) dovrebbero essere soddisfatti i criteri specifici di conformità stabiliti nell'allegato in relazione a ciascuna raccomandazione.

3. **Tempistica per dare seguito alla raccomandazione**

A norma dell'articolo 17, paragrafo 1, del regolamento (UE) n. 1092/2010, i destinatari devono comunicare al Parlamento europeo, al Consiglio, alla Commissione e al CERS le azioni intraprese in risposta alla presente raccomandazione o motivare un'eventuale inazione. Si richiede ai destinatari di presentare tale comunicazione secondo la seguente tempistica:

1. Raccomandazione A

(a) Entro il 30 giugno 2023, ma non prima di sei mesi dall'entrata in vigore del regolamento DORA, le AEV sono tenute a presentare al Parlamento europeo, al Consiglio, alla Commissione e al CERS una relazione intermedia sull'attuazione della sotto-raccomandazione A(1).

(b) Entro il 30 giugno 2024, ma non prima di diciotto mesi dall'entrata in vigore del regolamento DORA, le AEV sono tenute a presentare al Parlamento europeo, al Consiglio, alla Commissione e al CERS una relazione finale sull'attuazione della sotto-raccomandazione A(1).

(c) Entro il 30 giugno 2025, ma non prima di trenta mesi dall'entrata in vigore del regolamento DORA, le AEV sono tenute a presentare al Parlamento europeo, al Consiglio, alla Commissione e al CERS una relazione sull'attuazione della sotto-raccomandazione A(2).

2. Raccomandazione B

Entro il 30 giugno 2023, ma non prima di sei mesi dall'entrata in vigore del regolamento DORA, le AEV sono tenute a presentare al Parlamento europeo, al Consiglio, alla Commissione e al CERS una relazione sull'attuazione della sotto-raccomandazione A(2).

3. Raccomandazione C

(a) Entro il 31 dicembre 2023, ma non prima di 12 mesi dall'entrata in vigore del regolamento DORA, la Commissione è tenuta a presentare al Parlamento europeo, al Consiglio e al CERS una relazione sull'attuazione della raccomandazione C in vista della relazione intermedia delle AEV conformemente alla sotto-raccomandazione A(1).

([37]) Reglamento (UE) no 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) no 648/2012 (GU L 176 del 27.6.2013, pag. 1)

([38]) Raccomandazione CERS/2011/3 del Comitato europeo per il rischio sistemico, del 22 dicembre 2011, relativa al mandato macroprudenziale delle autorità nazionali (GU C 41 del 14.2.2012, pag. 1).

(b) Entro il 31 dicembre 2025, ma non prima di 36 mesi dall'entrata in vigore del regolamento DORA, la Commissione è tenuta a presentare al Parlamento europeo, al Consiglio e al CERS una relazione sull'attuazione della raccomandazione C in vista delle relazioni delle AEV conformemente alla sotto-raccomandazione A(1).

4. **Monitoraggio e valutazione**

1. Il segretariato del CERS:

(a) presterà assistenza ai destinatari, assicurando il coordinamento nella presentazione delle relazioni e la fornitura dei relativi modelli, nonché precisando, ove necessario, le modalità e la tempistica con cui dar seguito alla raccomandazione;

(b) verificherà il seguito dato dai destinatari, fornirà loro assistenza su richiesta e presenterà relazioni di follow-up al Consiglio generale. Le valutazioni saranno avviate secondo le seguenti modalità:

(i) entro 12 mesi dall'entrata in vigore del regolamento DORA per quanto riguarda l'attuazione delle raccomandazioni A e B;

(ii) entro 18 mesi dall'entrata in vigore del regolamento DORA per quanto riguarda l'attuazione della raccomandazione C;

(iii) entro 24 mesi dall'entrata in vigore del regolamento DORA per quanto riguarda l'attuazione della raccomandazione A;

(iv) entro 36 mesi dall'entrata in vigore del regolamento DORA per quanto riguarda l'attuazione della raccomandazione A;

(v) entro 42 mesi dall'entrata in vigore del regolamento DORA per quanto riguarda l'attuazione della raccomandazione C;

2. Il Consiglio generale valuterà le azioni e le motivazioni comunicate dai destinatari e, se del caso, può decidere che la presente raccomandazione non sia stata rispettata e che un destinatario abbia omesso di fornire adeguate motivazioni per la propria inerzia.

Fatto a Francoforte sul Meno, il 2 dicembre 2021

Il capo del segretariato del CERS,
per conto del Consiglio generale del CERS
Francesco MAZZAFERRO

ALLEGATO

SPECIFICAZIONE DEI CRITERI DI CONFORMITÀ APPLICABILI ALLE RACCOMANDAZIONI

Raccomandazione A — Istituzione di un quadro paneuropeo di coordinamento sistemico degli incidenti informatici (EU-SCICF)

Per la sotto-raccomandazione A, si definiscono i seguenti criteri di conformità.

1. Nel preparare una risposta coordinata efficace a livello dell'Unione che dovrebbe comportare lo sviluppo graduale dell'EU-SCICF esercitando il potere previsto dal futuro regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario (di seguito «DORA»), le autorità europee di vigilanza (AEV), agendo tramite il Comitato congiunto, insieme alla Banca centrale europea (BCE), al Comitato europeo per il rischio sistemico (CERS) e alle autorità nazionali competenti, e in consultazione con l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione e la Commissione, ove ritenuto necessario, dovrebbero prendere in considerazione la possibilità di includere nella prevista preparazione dell'UE-SCICF almeno i seguenti aspetti:

   a. analisi del fabbisogno di risorse per uno sviluppo efficace dell'EU-SCICF;

   b. sviluppo di esercitazioni di gestione delle crisi e delle emergenze che includano scenari di attacco informatico nell'ottica dello sviluppo di canali di comunicazione;

   c. sviluppo di un vocabolario comune;

   d. sviluppo di una classificazione coerente degli incidenti informatici;

   e. creazione di canali sicuri e affidabili per la condivisione delle informazioni, compresi i sistemi di back-up;

   f. istituzione di punti di contatto;

   g. affrontare la questione della riservatezza nella condivisione delle informazioni;

   h. iniziative di collaborazione e condivisione di informazioni con l'intelligence informatica del settore finanziario;

   i. sviluppo di processi di attivazione e di escalation efficaci attraverso la consapevolezza situazionale;

   j. chiarimento delle responsabilità dei partecipanti al quadro;

   k. sviluppo di interfacce per il coordinamento intersettoriale e, se del caso, con i paesi terzi;

   l. garantire una comunicazione coerente con il pubblico da parte delle autorità competenti per preservare la fiducia;

   m. creazione di linee di comunicazione predefinite per una comunicazione tempestiva;

   n. svolgimento di adeguati esercizi di verifica quadro, compresi test intergiurisdizionali e coordinamento con i paesi terzi, e valutazioni che si traducano in insegnamenti appresi ed evoluzione del quadro di riferimento;

   o. garantire una comunicazione e contromisure efficaci contro la disinformazione.

Raccomandazione B — Istituzione di punti di contatto dell'EU-SCICF

Per la raccomandazione B, si definiscono i seguenti criteri di conformità.

1. Le AEV, la BCE e ciascuno Stato membro tra le rispettive autorità nazionali competenti dovrebbero concordare un approccio comune alla condivisione e all'aggiornamento dell'elenco dei punti di contatto designati dell'EU-SCICF.

2. La designazione del punto di contatto dovrebbe essere valutata tenendo conto del punto di contatto unico designato a norma della direttiva (UE) 2016/1148 che gli Stati membri hanno istituito rispetto alla sicurezza delle reti e dei sistemi informativi per garantire la cooperazione transfrontaliera con gli altri Stati membri e con il gruppo di cooperazione in materia di reti e sistemi informativi.

Raccomandazione C – Modifiche al quadro giuridico dell'Unione

Per la raccomandazione C, si definisce il seguente criterio di conformità.

La Commissione dovrebbe valutare se, a seguito dell'analisi effettuata conformemente alla raccomandazione A, siano necessarie misure, comprese modifiche della pertinente legislazione dell'Unione, per garantire che le AEV, tramite il Comitato congiunto e insieme alla BCE, al CERS e alle autorità nazionali competenti, possano sviluppare l'EU-SCICF conformemente alla sotto-raccomandazione A(1) e per garantire che le AEV, la BCE, il CERS e le autorità nazionali competenti, nonché altre autorità, possano intraprendere azioni di coordinamento e scambio di informazioni sufficientemente dettagliati e coerenti da sostenere un efficace EU-SCICF.