Gazzetta ufficiale dell'Unione europea L 333

Edizione in lingua italiana

Legislazione

65° anno

27 dicembre 2022

Sommario

I *Atti legislativi*

REGOLAMENTI

★ **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] 1

DIRETTIVE

★ **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)** [1] 80

★ **Direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario** [1] 153

★ **Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio** [1] 164

[1] Testo rilevante ai fini del SEE.

IT

Gli atti i cui titoli sono stampati in caratteri chiari appartengono alla gestione corrente. Essi sono adottati nel quadro della politica agricola e hanno generalmente una durata di validità limitata.

I titoli degli altri atti sono stampati in grassetto e preceduti da un asterisco.

I

(Atti legislativi)

REGOLAMENTI

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

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea ([1]),

visto il parere del Comitato economico e sociale europeo ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) Nell'era digitale le tecnologie dell'informazione e della comunicazione (TIC) sostengono sistemi complessi impiegati nelle attività quotidiane. Mantengono in funzione i principali settori delle nostre economie, tra cui il settore finanziario, e migliorano il funzionamento del mercato interno. Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte i rischi informatici, rendendo l'intera società, e in particolare il sistema finanziario, più vulnerabile alle minacce informatiche o alle perturbazioni delle TIC. L'uso onnipresente dei sistemi di TIC e l'elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali delle attività delle entità finanziarie dell'Unione, ma la loro resilienza digitale deve ancora essere affrontata e integrata in maniera più efficace nei loro quadri operativi di portata più ampia.

(2) Negli ultimi decenni, l'uso delle TIC ha conquistato un ruolo essenziale nella fornitura di servizi finanziari, al punto da acquisire oggi un'importanza critica nell'esecuzione delle consuete funzioni quotidiane di tutte le entità finanziarie. Ora la digitalizzazione riguarda ad esempio i pagamenti, che stanno progressivamente migrando dal contante e dal cartaceo verso soluzioni digitali, nonché la compensazione e il regolamento dei titoli, la negoziazione elettronica e algoritmica, le operazioni di prestito e finanziamento, la finanza tra pari (*peer–to–peer finance*), i rating del credito, la gestione dei crediti e le operazioni di back-office. Anche il settore assicurativo è stato trasformato

([1]) GU C 343 del 26.8.2021, pag. 1.
([2]) GU C 155 del 30.4.2021, pag. 38.
([3]) Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.

dall'uso delle TIC, dall'emergere di intermediari assicurativi che offrono i loro servizi online e che operano con InsurTech fino alla sottoscrizione di assicurazioni digitali. Non solo l'intero settore finanziario è diventato in larga misura digitale, ma la digitalizzazione ha anche reso più marcate le interconnessioni e le dipendenze all'interno del settore e nei confronti di fornitori terzi di infrastrutture e servizi.

(3) In una relazione del 2020 incentrata sul rischio informatico sistemico, il Comitato europeo per il rischio sistemico (CERS) ha ribadito che l'attuale elevato livello di interconnessione tra entità finanziarie, mercati finanziari e infrastrutture del mercato finanziario, e in particolare l'interdipendenza dei rispettivi sistemi di TIC, potrebbe costituire una potenziale vulnerabilità sistemica dal momento che incidenti informatici localizzati potrebbero rapidamente diffondersi da una qualunque delle circa 22 000 entità finanziarie dell'Unione all'intero sistema finanziario, senza trovare alcun ostacolo nelle frontiere geografiche. Gravi violazioni delle TIC che si verifichino nel settore finanziario non si limitano a colpire entità finanziarie isolate, bensì spianano anche la strada alla propagazione di vulnerabilità localizzate attraverso tutti i canali di trasmissione finanziaria e possono provocare conseguenze avverse per la stabilità del sistema finanziario dell'Unione, dando luogo ad esempio a pressanti richieste di rimborsi e a una generale perdita di fiducia nei mercati finanziari.

(4) Negli ultimi anni, i rischi informatici hanno richiamato l'attenzione di responsabili politici e organismi di regolamentazione e normazione che, a livello nazionale, dell'Unione e internazionale, hanno cercato di migliorare la resilienza digitale, stabilire norme e coordinare il lavoro di regolamentazione o vigilanza. A livello internazionale, il comitato di Basilea per la vigilanza bancaria, il comitato per i pagamenti e le infrastrutture di mercato, il consiglio per la stabilità finanziaria, l'istituto per la stabilità finanziaria, nonché il G7 e il G20, si propongono di fornire alle autorità competenti e agli operatori del mercato di varie giurisdizioni gli strumenti per potenziare la resilienza dei rispettivi sistemi finanziari. Tale lavoro è stato inoltre dettato dalla necessità di tenere debitamente conto dei rischi informatici nel contesto di un sistema finanziario globale altamente interconnesso e di perseguire una maggiore coerenza delle migliori prassi pertinenti.

(5) Benché a livello dell'Unione e nazionale siano state adottate iniziative politiche e legislative mirate, i rischi informatici continuano a rappresentare una sfida per la resilienza operativa, le prestazioni e la stabilità del sistema finanziario dell'Unione. Le riforme che sono state introdotte sulla scia della crisi finanziaria del 2008 hanno rafforzato in primo luogo la resilienza finanziaria del settore finanziario dell'Unione, mirando a salvaguardare la competitività e la stabilità dell'Unione in una prospettiva economica, prudenziale e di condotta sul mercato. Benché si inseriscano nel quadro del rischio operativo, la sicurezza delle TIC e la resilienza digitale hanno occupato un posto meno rilevante nell'agenda normativa dopo la crisi finanziaria e sono state potenziate solo in alcuni settori del panorama delle politiche e della normativa dell'Unione in materia di servizi finanziari, o soltanto in alcuni Stati membri.

(6) Nella comunicazione del 8 marzo 2018 intitolata «Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo» la Commissione ha sottolineato la fondamentale importanza di una maggiore resilienza del settore finanziario dell'Unione, anche da un punto di vista operativo, allo scopo di garantirne il buon funzionamento e la sicurezza tecnologica nonché la rapida ripresa dopo incidenti e violazioni delle TIC, consentendo in ultima analisi la fornitura efficace e ordinata dei servizi finanziari in tutta l'Unione, anche in situazioni di stress, preservando nel contempo la fiducia dei consumatori e degli operatori del mercato.

(7) Nell'aprile 2019 l'Autorità europea di vigilanza (Autorità bancaria europea — ABE), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([4]), l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali — EIOPA) istituita dal regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([5]) e l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati — ESMA) istituita dal regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([6])

([4]) 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).

([5]) 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).

([6]) 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).

(denominate collettivamente «autorità europee di vigilanza» o «AEV») hanno pubblicato congiuntamente pareri tecnici in cui si invocava l'adozione di un approccio coerente ai rischi informatici nel settore finanziario e si raccomandava di potenziare, in maniera proporzionata, la resilienza operativa digitale del settore dei servizi finanziari tramite un'iniziativa settoriale dell'Unione.

(8) Il settore finanziario dell'Unione è regolamentato da un codice unico ed è disciplinato da un sistema europeo di vigilanza finanziaria. Le disposizioni sulla resilienza operativa digitale e sulla sicurezza delle TIC non sono tuttavia ancora armonizzate in maniera completa o coerente, benché nell'era digitale la resilienza operativa digitale sia un elemento fondamentale della stabilità finanziaria e dell'integrità del mercato, non meno importante, ad esempio, delle norme comuni riguardanti gli aspetti prudenziali o la condotta sul mercato. Sarebbe quindi opportuno perfezionare il codice unico e il sistema di vigilanza per coprire anche la resilienza operativa digitale, rafforzando i mandati delle autorità competenti per consentire loro di vigilare sulla gestione dei rischi informatici nel settore finanziario al fine di proteggere l'integrità e l'efficienza del mercato interno ed agevolarne il regolare funzionamento.

(9) Le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza a livello nazionale per quanto riguarda i rischi informatici ostacolano il funzionamento del mercato interno dei servizi finanziari e intralciano il regolare esercizio della libertà di stabilimento e la libera prestazione di servizi per le entità finanziarie che operano su base transfrontaliera. Potrebbe risultarne falsata anche la concorrenza tra entità finanziarie dello stesso tipo attive in Stati membri diversi. È quanto accade in particolare nei settori in cui l'armonizzazione a livello di Unione è stata assai limitata, come i test di resilienza operativa digitale, o assente, come il monitoraggio dei rischi informatici derivanti da terzi. Le disparità provocate dagli sviluppi previsti a livello nazionale potrebbero produrre ostacoli ulteriori al funzionamento del mercato interno, a danno dei partecipanti al mercato e della stabilità finanziaria.

(10) Ad oggi, dal momento che le disposizioni sui rischi informatici sono state trattate in modo soltanto parziale a livello di Unione, esistono carenze o sovrapposizioni in settori importanti, come la segnalazione degli incidenti connessi alle TIC e i test di resilienza operativa digitale, nonché incoerenze dovute alla divergenza delle norme nazionali o al sovrapporsi di norme la cui applicazione risulta inefficiente sotto il profilo dei costi. Si tratta di una situazione particolarmente dannosa per un settore come quello finanziario, che si contraddistingue per l'intenso ricorso alle TIC poiché i rischi tecnologici non conoscono frontiere e il settore finanziario offre i suoi servizi su base transfrontaliera sia all'interno che all'esterno dell'Unione. Le singole entità finanziarie che sono attive a livello transfrontaliero o detengono varie autorizzazioni (ad esempio, un'entità finanziaria può detenere autorizzazioni a operare quale banca, impresa di investimento e istituto di pagamento, ciascuna delle quali rilasciata da una diversa autorità competente in uno o più Stati membri) devono superare autonomamente sfide operative poste dai rischi informatici e dalla necessità di mitigare gli impatti avversi degli incidenti connessi alle TIC in maniera coerente ed efficiente sotto il profilo dei costi.

(11) Dal momento che il codice unico non è accompagnato da un quadro generale per i rischi informatici o operativi, è necessario armonizzare ulteriormente i principali obblighi in materia di resilienza operativa digitale per tutte le entità finanziarie. Lo sviluppo delle capacità delle TIC e della resilienza complessiva da parte delle entità finanziarie, sulla base di tali obblighi fondamentali, al fine di far fronte ad interruzioni operative, contribuirebbe a preservare la stabilità e l'integrità dei mercati finanziari dell'Unione e perciò a mantenere elevato il livello di protezione degli investitori e dei consumatori nell'Unione. Poiché il presente regolamento si propone di contribuire al regolare funzionamento del mercato interno, dovrebbe basarsi sulle disposizioni dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE) interpretate conformemente alla giurisprudenza costante della Corte di giustizia dell'Unione europea (Corte di giustizia).

(12) Il presente regolamento mira a consolidare e aggiornare i requisiti in materia di rischi informatici nell'ambito dei requisiti in materia di rischi operativi che sono state finora trattati separatamente in vari atti giuridici dell'Unione. Tali atti riguardavano le principali categorie di rischio finanziario (ad esempio rischio di credito, rischio di mercato, rischio di controparte e rischio di liquidità, rischio di condotta sul mercato), ma nel momento in cui sono stati adottati non trattavano in maniera globale tutte le componenti della resilienza operativa. Le norme sui rischi operativi ulteriormente sviluppate in tali atti giuridici dell'Unione hanno sovente privilegiato il tradizionale approccio quantitativo alla gestione dei rischi (ossia la definizione di un requisito patrimoniale a copertura dei rischi

informatici) rispetto a norme qualitative mirate concernenti le capacità di protezione, individuazione, contenimento, ripristino e rimedio in relazione agli incidenti connessi alle TIC, oppure le capacità di segnalazione e test digitali. Tali atti si prefiggevano principalmente lo scopo di trattare e aggiornare le norme fondamentali in materia di vigilanza prudenziale e integrità o condotta sul mercato. Tramite il consolidamento e l'aggiornamento delle diverse norme sui rischi informatici, tutte le disposizioni in materia di rischio digitale nel settore finanziario dovrebbero essere coerentemente riunite per la prima volta in un unico atto legislativo. Il presente regolamento colma pertanto le lacune o pone rimedio alle incoerenze di taluni fra i precedenti atti legislativi, anche per quanto riguarda la terminologia utilizzata, e fa esplicito riferimento ai rischi informatici tramite norme specifiche in materia di capacità di gestione dei rischi informatici, segnalazione degli incidenti, test di resilienza operativa e monitoraggio dei rischi informatici derivanti da terzi. Pertanto il presente regolamento dovrebbe altresì accrescere la consapevolezza dei rischi informatici e riconoscere che gli incidenti connessi alle TIC e la mancanza di resilienza operativa potrebbero compromettere la solidità delle entità finanziarie.

(13) Nell'affrontare i rischi informatici è opportuno che le entità finanziarie seguano lo stesso approccio e le stesse norme basate su principi, tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività. La coerenza contribuisce ad accrescere la fiducia nel sistema finanziario e a preservarne la stabilità, soprattutto in tempi in cui l'elevata dipendenza da infrastrutture, piattaforme e sistemi di TIC comporta maggiori rischi digitali. Il rispetto dei fondamenti per la sicurezza dei sistemi TIC (*basic cyber hygiene*) dovrebbe anche evitare l'imposizione di costi elevati per l'economia, riducendo al minimo l'impatto e i costi delle perturbazioni a livello di TIC.

(14) I regolamenti servono a ridurre la complessità normativa, favoriscono la convergenza della vigilanza, incrementano la certezza del diritto e contribuiscono altresì a limitare i costi di conformità, specialmente per le entità finanziarie che operano a livello transfrontaliero, e a ridurre le distorsioni della concorrenza. Pertanto, la scelta di un regolamento per istituire un quadro comune sulla resilienza operativa digitale delle entità finanziarie costituisce il metodo più idoneo per garantire l'applicazione omogenea e coerente di tutte le componenti della gestione dei rischi informatici da parte del settore finanziario dell'Unione.

(15) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([7]) ha rappresentato il primo quadro orizzontale per la cibersicurezza adottato a livello di Unione, che si applica anche a tre tipi di entità finanziarie, ossia enti creditizi, sedi di negoziazione e controparti centrali. Dal momento però che la direttiva (UE) 2016/1148 ha introdotto un meccanismo di identificazione a livello nazionale per gli operatori di servizi essenziali, solo alcuni enti creditizi, sedi di negoziazione e controparti centrali che sono stati identificati dagli Stati membri e rientrano in concreto nel suo ambito di applicazione e sono quindi tenuti a rispettare gli obblighi in materia di notifica degli incidenti e sicurezza connessi alle TIC contenute nella direttiva stessa. La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([8]) stabilisce un criterio uniforme per stabilire quali entità rientrano nel suo ambito di applicazione (regola della soglia di dimensione), mantenendo nel contempo in tale ambito di applicazione anche i tre tipi di entità finanziarie.

(16) Tuttavia, dal momento che il presente regolamento accresce il livello di armonizzazione delle varie componenti della resilienza digitale, introducendo requisiti in materia di gestione dei rischi informatici e segnalazione di incidenti connessi alle TIC più rigorosi rispetto a quelli contenuti nell'attuale normativa dell'Unione in materia di servizi finanziari, questo livello più elevato determina un incremento dell'armonizzazione anche rispetto ai requisiti di cui alla direttiva (UE) 2022/2555. Di conseguenza, il presente regolamento costituisce una *lex specialis* rispetto alla direttiva (UE) 2022/2555. Al tempo stesso, è essenziale mantenere un saldo rapporto tra il settore finanziario e il quadro orizzontale di cibersicurezza dell'Unione, come attualmente stabilito nella direttiva (UE) 2022/2555, per garantire la coerenza con le strategie di cibersicurezza adottate dagli Stati membri e permettere alle autorità di vigilanza finanziaria di venire a conoscenza degli incidenti informatici che colpiscono altri settori contemplati da tale direttiva.

([7]) 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).

([8]) 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, che modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (cfr. pag. 80 della presente Gazzetta ufficiale).

(17) A norma dell'articolo 4, paragrafo 2, del trattato sull'Unione europea e fatto salvo il controllo giurisdizionale della Corte di giustizia, il presente regolamento non dovrebbe pregiudicare la responsabilità degli Stati membri in relazione a funzioni essenziali dello Stato riguardanti la sicurezza pubblica, la difesa e la tutela della sicurezza nazionale, ad esempio per quanto riguarda la fornitura di informazioni che sarebbero contrarie alla tutela della sicurezza nazionale.

(18) Per consentire l'apprendimento intersettoriale e attingere efficacemente alle esperienze di altri settori nella lotta alle minacce informatiche, le entità finanziarie di cui alla direttiva (UE) 2022/2555 dovrebbero continuare a far parte dell'«ecosistema» di quella direttiva [ad esempio il gruppo di cooperazione e i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)]. Le AEV e le autorità nazionali competenti dovrebbero poter partecipare alle discussioni strategiche delle politiche e ai lavori tecnici del gruppo di cooperazione ai sensi della direttiva, nonché scambiare informazioni e cooperare maggiormente con i punti di contatto unici designati o istituiti in conformità di tale direttiva. Le autorità competenti previste dal presente regolamento dovrebbero anche consultare i CSIRT e collaborare con loro. Le autorità competenti dovrebbero inoltre poter chiedere il parere tecnico delle autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 e concludere accordi di cooperazione volti a garantire meccanismi di coordinamento efficaci e di risposta rapida.

(19) Date le forti interconnessioni tra la resilienza digitale e la resilienza fisica delle entità finanziarie, nel presente regolamento e nella direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio ([9]) è necessario seguire un approccio coerente per quanto riguarda la resilienza dei soggetti critici. Dato che la resilienza fisica delle entità finanziarie è affrontata in modo globale dagli obblighi di gestione dei rischi informatici e di segnalazione disciplinati dal presente regolamento, gli obblighi di cui ai capi III e IV della direttiva (UE) 2022/2557 non dovrebbero applicarsi alle entità finanziarie che rientrano nell'ambito di applicazione di tale direttiva.

(20) I fornitori di servizi di cloud computing sono una delle categorie di infrastrutture digitali contemplate dalla direttiva (UE) 2022/2555. Il quadro di sorveglianza dell'Unione (quadro di sorveglianza) istituito dal presente regolamento si applica a tutti i fornitori terzi critici di servizi TIC, compresi i fornitori di servizi di cloud computing che forniscono servizi TIC a entità finanziarie, e dovrebbe essere considerato complementare alla vigilanza condotta ai sensi della direttiva (UE) 2022/2555. Inoltre, in assenza di un quadro orizzontale dell'Unione che istituisca un'autorità per la sorveglianza digitale, il quadro di sorveglianza istituito dal presente regolamento dovrebbe estendersi ai fornitori di servizi di cloud computing.

(21) Al fine di mantenere il pieno controllo sui rischi informatici, le entità finanziarie devono dotarsi di capacità generali per consentire una gestione dei rischi informatici forte ed efficace, nonché di politiche e meccanismi specifici per il trattamento di tutti gli incidenti connessi alle TIC e per la segnalazione degli incidenti più gravi connessi alle TIC. Analogamente, le entità finanziarie dovrebbero dotarsi di politiche per i test su processi, controlli e sistemi di TIC nonché per la gestione dei rischi informatici derivanti da terzi. È opportuno potenziare la resilienza operativa digitale di base per le entità finanziarie, consentendo tuttavia anche un'applicazione proporzionata dei requisiti a carico di talune entità finanziarie, in particolare le microimprese, così come le entità finanziarie soggette a un quadro semplificato per la gestione dei rischi informatici. Per agevolare una vigilanza efficace degli enti pensionistici aziendali o professionali che sia proporzionata e risponda alla necessità di ridurre gli oneri amministrativi a carico delle autorità competenti, le pertinenti disposizioni nazionali in materia di vigilanza applicabili a tali entità finanziarie dovrebbero tenere conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività, anche in caso di superamento delle soglie pertinenti di cui all'articolo 5 della direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio ([10]). In particolare, le attività di vigilanza dovrebbero concentrarsi principalmente sulla necessità di affrontare i rischi gravi associati alla gestione dei rischi informatici di un'entità specifica.

([9]) Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (cfr. pag. 164 della presente Gazzetta ufficiale).

([10]) 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).

Le autorità competenti dovrebbero inoltre mantenere un approccio vigile ma proporzionato in relazione alla vigilanza degli enti pensionistici aziendali o professionali che, conformemente all'articolo 31 della direttiva (UE) 2016/2341, esternalizzano a fornitori di servizi una parte significativa delle loro attività principali, quali la gestione patrimoniale, i calcoli attuariali, la contabilità e la gestione dei dati.

(22) Le soglie e le tassonomie per la segnalazione degli incidenti connessi alle TIC variano sensibilmente a livello nazionale. È possibile trovare un terreno comune grazie al lavoro compiuto in materia dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) istituita dal regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([11]) e dal gruppo di cooperazione istituito ai sensi della direttiva (UE) 2022/2555, ma in merito alla fissazione delle soglie e all'uso delle tassonomie si registrano ancora o possono emergere divergenze di approcci per le altre entità finanziarie. A causa di tali divergenze, vi sono una molteplicità di requisiti che le entità finanziarie devono rispettare, soprattutto quando operano in vari Stati membri oppure quando fanno parte di un gruppo finanziario. Inoltre, tali divergenze possono potenzialmente ostacolare la creazione di nuovi meccanismi uniformi o centralizzati dell'Unione che accelerano il processo di segnalazione e coadiuvano uno scambio di informazioni rapido e regolare tra le autorità competenti: elemento essenziale, quest'ultimo, per affrontare i rischi informatici nell'eventualità di attacchi su vasta scala con conseguenze potenzialmente sistemiche.

(23) Al fine di ridurre gli oneri amministrativi e la potenziale duplicazione degli obblighi di segnalazione per talune entità finanziarie, l'obbligo di segnalazione degli incidenti a norma della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio ([12]) dovrebbe cessare di applicarsi ai prestatori di servizi di pagamento che rientrano nell'ambito di applicazione del presente regolamento. Di conseguenza, gli enti creditizi, gli istituti di moneta elettronica, gli istituti di pagamento e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, di tale direttiva, dovrebbero, a decorrere dalla data di applicazione del presente regolamento, segnalare a norma del presente regolamento tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti che sono stati precedentemente segnalati a norma di tale direttiva, indipendentemente dal fatto che si tratti di incidenti connessi alle TIC.

(24) Per consentire alle autorità competenti di assolvere le funzioni di vigilanza acquisendo un panorama completo di natura, frequenza, rilevanza e impatto degli incidenti connessi alle TIC e per agevolare lo scambio di informazioni tra le autorità pubbliche competenti, comprese le autorità di contrasto e le autorità di risoluzione, il presente regolamento dovrebbe stabilire un solido regime di segnalazione degli incidenti connessi alle TIC in base ai cui requisiti sarebbero colmate le attuali lacune della normativa in materia di servizi finanziari ed eliminate le sovrapposizioni e le duplicazioni esistenti in modo da diminuire i costi. È essenziale armonizzare il regime di segnalazione degli incidenti connessi alle TIC chiedendo a tutte le entità finanziarie di riferire alle rispettive autorità competenti attraverso il quadro unico semplificato stabilito nel presente regolamento. Alle AEV si dovrebbe poi conferire il potere di precisare ulteriormente gli elementi pertinenti del quadro per la segnalazione degli incidenti connessi alle TIC come la tassonomia, i limiti temporali, le serie di dati, i modelli e le soglie applicabili. Per garantire la piena coerenza con la direttiva (UE) 2022/2555, alle entità finanziarie dovrebbe essere consentito, su base volontaria, di notificare all'autorità competente interessata le minacce informatiche significative qualora ritengano che la minaccia informatica sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti.

(25) In taluni sottosettori finanziari sono stati elaborati requisiti in materia di test di resilienza operativa digitale che stabiliscono quadri che non sono sempre pienamente allineati. Ne è scaturita una potenziale duplicazione di costi per le entità finanziarie transfrontaliere, che rende complesso il reciproco riconoscimento dei risultati dei test di resilienza operativa digitale, il che a sua volta può frammentare il mercato interno.

([11]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15).

([12]) 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).

(26) Inoltre, qualora non si richiedano test relativi alle TIC, le vulnerabilità non sono individuate ed espongono quindi un'entità finanziaria a rischi informatici e, in ultima analisi, creano un rischio più elevato per la stabilità e l'integrità del settore finanziario. Senza un intervento dell'Unione, i test in materia di resilienza operativa digitale continuerebbero a essere incoerenti e non disporrebbero di un sistema di riconoscimento reciproco dei risultati dei test informatici fra le diverse giurisdizioni. È inoltre improbabile che altri sottosettori finanziari adottino regimi di test su scala significativa; pertanto essi si lascerebbero sfuggire i potenziali benefici di un quadro in materia di test, in termini di individuazione di vulnerabilità e rischi informatici, e verifica delle capacità di difesa e della continuità operativa, che contribuisca ad aumentare la fiducia di clienti, fornitori e partner commerciali. Per porre rimedio a tali sovrapposizioni, divergenze e carenze è necessario stabilire norme per un regime coordinato di test e agevolare così il riconoscimento reciproco dei test avanzati per le entità finanziarie che soddisfino i criteri di cui al presente regolamento.

(27) La dipendenza delle entità finanziarie dall'uso dei servizi TIC è causata in parte dalla loro necessità di adattarsi all'emergere di un'economia mondiale digitale sempre più competitiva, di accrescere la propria efficienza commerciale e di soddisfare la domanda dei consumatori. La natura e la portata di tale dipendenza ha conosciuto negli ultimi anni un'evoluzione costante, che ha prodotto una riduzione dei costi dell'intermediazione finanziaria, ha favorito l'espansione e la scalabilità delle imprese nello sviluppo delle attività finanziarie, offrendo d'altra parte un'ampia gamma di strumenti TIC per la gestione di complessi processi interni.

(28) Tale ampio uso dei servizi TIC è testimoniato dalla complessità degli accordi contrattuali: le entità finanziarie incontrano spesso difficoltà nel negoziare condizioni contrattuali che siano conformi a norme prudenziali o ad altri requisiti normativi cui sono sottoposte oppure nell'applicare diritti specifici, quali i diritti di accesso o di audit, anche quando tali diritti siano previsti nei loro accordi contrattuali. Inoltre, molti di tali accordi contrattuali non contengono salvaguardie sufficienti per il monitoraggio esauriente dei processi di subappalto, e privano in tal modo l'entità finanziaria della capacità di valutare i rischi associati. Inoltre, dal momento che i fornitori terzi di servizi TIC spesso offrono servizi standardizzati a una clientela differenziata, tali accordi contrattuali non sono sempre idonei a soddisfare le esigenze individuali o specifiche dei soggetti del settore finanziario.

(29) Anche se il diritto dell'Unione in materia di servizi finanziari contiene talune norme generali in materia di esternalizzazione, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato nel diritto dell'Unione. In assenza di norme dell'Unione che si applichino in maniera chiara e mirata alle disposizioni contrattuali stipulate con fornitori terzi di servizi TIC, la fonte esterna dei rischi informatici rimane una questione non adeguatamente affrontata. È pertanto necessario stabilire alcuni principi fondamentali che indirizzino la gestione, da parte delle entità finanziarie, dei rischi informatici derivanti da terzi, che sono di particolare importanza quando le entità finanziarie ricorrono a fornitori terzi di servizi TIC a supporto delle loro funzioni essenziali o importanti. Tali principi dovrebbero essere accompagnati da una serie di diritti contrattuali di base concernenti vari elementi dell'esecuzione e della risoluzione degli accordi contrattuali, al fine di fornire alcune garanzie minime per rafforzare la capacità delle entità finanziarie di monitorare efficacemente tutti i rischi informatici che insorgano a livello di fornitori di servizi terzi. Tali principi sono complementari alla normativa settoriale applicabile all'esternalizzazione.

(30) Oggi è evidente una certa carenza di omogeneità e convergenza per quanto riguarda il monitoraggio delle dipendenze da terzi nel settore delle TIC e dei rischi informatici derivanti da terzi. Nonostante gli sforzi per trattare l'esternalizzazione, come gli orientamenti dell'ABE in materia di esternalizzazione del 2019 e degli orientamenti dell'ESMA in materia di esternalizzazione a fornitori di servizi cloud del 2021, la questione più ampia del contrasto del rischio sistemico potenzialmente derivante dall'esposizione del settore finanziario a un ristretto numero di fornitori terzi critici di servizi TIC non è adeguatamente affrontata dal diritto dell'Unione. La carenza di norme a livello dell'Unione è aggravata dall'assenza di norme nazionali su strumenti e mandati che consentano alle autorità di vigilanza finanziaria di acquisire una valida comprensione delle dipendenze da terzi nel settore delle TIC e di monitorare adeguatamente i rischi provocati dalla concentrazione di tali dipendenze.

(31) Tenendo presenti i potenziali rischi sistemici derivanti dalla diffusione delle pratiche di esternalizzazione e dalla concentrazione dei servizi TIC forniti da terzi, e alla luce dell'inadeguatezza dei meccanismi nazionali nel fornire alle autorità di vigilanza finanziaria strumenti adeguati per quantificare, qualificare e rettificare le conseguenze dei rischi informatici che interessano i fornitori terzi critici di servizi TIC, è necessario stabilire un adeguato quadro di sorveglianza che preveda il monitoraggio costante delle attività di quei fornitori terzi di servizi TIC che sono fornitori terzi critici di servizi TIC per le entità finanziarie, garantendo nel contempo la riservatezza e la sicurezza dei clienti diversi dalle entità finanziarie. Sebbene la fornitura intragruppo di servizi TIC comporti rischi e benefici specifici, essa non dovrebbe essere automaticamente considerata meno rischiosa della fornitura di servizi TIC da parte di fornitori al di fuori di un gruppo finanziario e dovrebbe pertanto essere soggetta allo stesso quadro normativo. Tuttavia, quando i servizi TIC sono forniti dall'interno dello stesso gruppo finanziario, le entità finanziarie potrebbero esercitare un livello di controllo più elevato sui fornitori intragruppo, il che dovrebbe essere preso in considerazione nella valutazione complessiva del rischio.

(32) Di fronte ai rischi informatici che si fanno sempre più complessi e sofisticati, la validità delle misure di individuazione e prevenzione dei rischi informatici dipende in larga misura da una costante condivisione delle analisi delle minacce e delle vulnerabilità tra le entità finanziarie. La condivisione delle informazioni contribuisce a creare una maggiore consapevolezza delle minacce informatiche. Ciò a sua volta accresce la capacità delle entità finanziarie di impedire che le minacce informatiche si trasformino in incidenti concreti connessi alle TIC e consente alle entità finanziarie di arginare in maniera più efficace l'impatto degli incidenti connessi alle TIC e di effettuare un ripristino più rapido. In assenza di orientamenti a livello di Unione, numerosi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di protezione dei dati, antitrust e responsabilità, hanno apparentemente ostacolato la condivisione dei dati.

(33) Inoltre i dubbi sul tipo di informazioni che è possibile condividere con altri partecipanti al mercato, o con autorità diverse da quelle di vigilanza (come l'ENISA per i contributi analitici o l'Europol per le attività di contrasto), possono determinare la mancata comunicazione di informazioni preziose. Le informazioni condivise rimangono quindi attualmente limitate e frammentate in termini quantitativi e qualitativi: gli scambi pertinenti avvengono per lo più a livello locale (tramite iniziative nazionali) e non esistono meccanismi di condivisione delle informazioni estesi in maniera omogenea a tutta l'Unione e corrispondenti alle esigenze di un sistema finanziario integrato. È pertanto importante rafforzare tali canali di comunicazione.

(34) È opportuno incoraggiare le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche e a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di valutare e monitorare adeguatamente le minacce informatiche, difendersi dai loro effetti e rispondervi, partecipando a meccanismi di condivisione delle informazioni. È perciò necessario consentire l'emergere a livello dell'Unione di meccanismi volontari di condivisione delle informazioni i quali, se attuati in ambienti sicuri, aiuterebbero la comunità del settore finanziario a prevenire le minacce informatiche e a rispondervi collettivamente, contenendo rapidamente la diffusione dei rischi informatici e impedendo il potenziale contagio tramite i canali finanziari. Tali meccanismi dovrebbero essere conformi alle norme del diritto dell'Unione vigenti in materia di concorrenza di cui alla comunicazione della Commissione del 14 gennaio 2011 intitolata «Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale» nonché alle norme dell'Unione sulla protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([13]). Essi dovrebbero operare sulla base del ricorso a una o più basi giuridiche stabilite all'articolo 6 di tale regolamento, ad esempio nel contesto del trattamento dei dati personali necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi dell'articolo 6, paragrafo 1, lettera f), dello stesso regolamento, nonché nel contesto del trattamento dei dati personali necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettere c) ed e), rispettivamente, di tale regolamento.

([13]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(35) Al fine di mantenere un elevato livello di resilienza operativa digitale per l'intero settore finanziario e al tempo stesso tenere il passo con gli sviluppi tecnologici, il presente regolamento dovrebbe affrontare i rischi derivanti da tutti i tipi di servizi TIC. A tal fine la definizione di servizi TIC nel contesto del presente regolamento dovrebbe essere intesa in senso lato e includere i servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa. Tale definizione dovrebbe includere, ad esempio, i cosiddetti servizi «over the top», che rientrano nella categoria dei servizi di comunicazione elettronica. Dovrebbe essere esclusa solo la limitata categoria dei servizi telefonici analogici tradizionali che possono essere considerati servizi di rete telefonica pubblica commutata (*Public Switched Telephone Network* — PSTN), servizi di rete terrestre, servizio telefonico tradizionale di base (*Plain Old Telephone Service* — POTS) o servizi di telefonia fissa.

(36) Nonostante l'ampia portata prevista dal presente regolamento, l'applicazione delle norme in materia di resilienza operativa digitale dovrebbe tener conto delle differenze significative che si registrano tra le entità finanziarie in termini di dimensioni e profilo di rischio complessivo. Come principio generale, al momento di distribuire risorse e capacità per l'attuazione del quadro per la gestione dei rischi informatici, le entità finanziarie dovrebbero trovare il giusto equilibrio tra le proprie esigenze nel campo delle TIC, da un lato, e le loro dimensioni e il loro profilo di rischio complessivo, nonché la natura, la portata e la complessità dei loro servizi, delle loro attività e della loro operatività, dall'altro; le autorità competenti dovrebbero invece valutare e riesaminare costantemente l'approccio che guida tale distribuzione.

(37) I prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366 rientrano esplicitamente nell'ambito di applicazione del presente regolamento, tenendo conto della natura specifica delle loro attività e dei rischi che ne derivano. Inoltre, gli istituti di moneta elettronica e gli istituti di pagamento esentati a norma dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE del Parlamento europeo e del Consiglio ([14]) e dell'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366 rientrano nell'ambito di applicazione del presente regolamento anche se non hanno ottenuto l'autorizzazione a norma della direttiva 2009/110/CE a emettere moneta elettronica o se non hanno ottenuto l'autorizzazione a norma della direttiva (UE) 2015/2366 a prestare ed eseguire servizi di pagamento. Tuttavia, gli uffici postali di cui all'articolo 2, paragrafo 5, punto 3), della direttiva 2013/36/UE del Parlamento europeo e del Consiglio ([15]) sono esclusi dall'ambito di applicazione del presente regolamento. L'autorità competente per gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366, gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366, dovrebbe essere l'autorità competente designata a norma dell'articolo 22 della direttiva (UE) 2015/2366.

(38) Poiché le entità finanziarie di maggiori dimensioni potrebbero disporre di maggiori risorse e possono destinare rapidamente fondi allo sviluppo di strutture di governance e all'elaborazione di varie strategie aziendali, è opportuno imporre l'introduzione di meccanismi di governance più complessi solo alle entità finanziarie che non sono microimprese ai sensi del presente regolamento. Tali entità sono meglio attrezzate, in particolare per istituire funzioni aziendali per la supervisione degli accordi con i fornitori terzi di servizi TIC o per affrontare la gestione delle crisi, per organizzare la loro gestione dei rischi informatici secondo il modello delle tre linee di difesa o ancora per stabilire un modello interno di controllo e gestione del rischio e sottoporre ad audit interni il proprio quadro per la gestione dei rischi informatici.

(39) Alcune entità finanziarie beneficiano di esenzioni o sono soggette a un quadro normativo meno rigoroso a norma della pertinente normativa settoriale dell'Unione. Tali entità finanziarie includono i gestori di fondi di investimento alternativi di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE del Parlamento europeo e del Consiglio ([16]), le imprese di assicurazione e di riassicurazione di cui all'articolo 4 della direttiva 2009/138/CE del Parlamento europeo e del Consiglio ([17]) e gli enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che

([14]) 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).

([15]) 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 e sulle imprese di investimento, 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).

([16]) 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).

([17]) 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).

contano congiuntamente non più di 15 aderenti in totale. Alla luce di tali esenzioni non sarebbe proporzionato includere tali entità finanziarie nell'ambito di applicazione del presente regolamento. Inoltre, il presente regolamento riconosce le specificità della struttura del mercato dell'intermediazione assicurativa, con la conseguenza che gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi a titolo accessorio che rientrano nella definizione di microimprese o di piccole o medie imprese non dovrebbero essere soggetti al presente regolamento.

(40) Poiché le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE sono escluse dall'ambito di applicazione di tale direttiva, gli Stati membri dovrebbero quindi poter scegliere di esentare dall'applicazione del presente regolamento tali entità situate nei rispettivi territori.

(41) Analogamente, al fine di allineare il presente regolamento all'ambito di applicazione della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([18]), è altresì opportuno escludere dall'ambito di applicazione del presente regolamento le persone fisiche e giuridiche di cui agli articoli 2 e 3 di tale direttiva che sono autorizzate a prestare servizi di investimento senza dover ottenere un'autorizzazione a norma della direttiva 2014/65/UE. Tuttavia l'articolo 2 della direttiva 2014/65/UE esclude anche dall'ambito di applicazione di tale direttiva le entità considerate entità finanziarie ai fini del presente regolamento, quali i depositari centrali di titoli, gli organismi d'investimento collettivo o le imprese di assicurazione e di riassicurazione. L'esclusione dall'ambito di applicazione del presente regolamento delle persone e delle entità di cui agli articoli 2 e 3 di tale direttiva non dovrebbe comprendere tali depositari centrali di titoli, organismi d'investimento collettivo o imprese di assicurazione e di riassicurazione.

(42) A norma del diritto settoriale dell'Unione, alcune entità finanziarie sono soggette a requisiti meno rigorosi o esenzioni per motivi legati alle loro dimensioni o ai servizi che forniscono. Tale categoria di entità finanziarie include le imprese di investimento piccole e non interconnesse, i piccoli enti pensionistici aziendali o professionali che possono essere esclusi dall'ambito di applicazione della direttiva (UE) 2016/2341 alle condizioni di cui all'articolo 5 di tale direttiva dallo Stato membro interessato e che gestiscono schemi pensionistici che contano congiuntamente non più di cento aderenti in totale, nonché gli enti esentati a norma della direttiva 2013/36/UE. Pertanto, conformemente al principio di proporzionalità e al fine di preservare lo spirito della normativa settoriale dell'Unione, è altresì opportuno che tali entità finanziarie siano soggette a un quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento. La proporzionalità del quadro per la gestione dei rischi informatici riguardante tali entità finanziarie non dovrebbe essere modificata dalle norme tecniche di regolamentazione che devono essere elaborate dalle AEV. Inoltre, conformemente al principio di proporzionalità, è opportuno che anche gli istituti di pagamento di cui all'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366 e gli istituti di moneta elettronica di cui all'articolo 9 della direttiva 2009/110/CE esentati conformemente al diritto nazionale che recepisce tali atti giuridici dell'Unione siano soggetti a un quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento, mentre gli istituti di pagamento e gli istituti di moneta elettronica che non sono stati esentati conformemente al rispettivo diritto nazionale che recepisce la normativa settoriale dell'Unione dovrebbero rispettare il quadro generale stabilito dal presente regolamento.

(43) Analogamente, le entità finanziarie che rientrano nella definizione di microimprese o sono soggette al quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento non dovrebbero essere tenute a istituire una funzione per il monitoraggio degli accordi conclusi con i fornitori terzi di servizi TIC per l'uso di tali servizi, o a designare un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente; ad attribuire la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo e garantire un adeguato livello di indipendenza di tale funzione per evitare conflitti d'interessi; a documentare e riesaminare almeno una volta all'anno il quadro per la gestione dei rischi informatici; a sottoporre ad audit interno periodico il quadro per la gestione dei rischi informatici; a svolgere valutazioni approfondite dopo modifiche di rilievo dei loro processi e delle loro infrastrutture di rete e dei sistemi informativi; a compiere periodicamente analisi dei rischi sui sistemi legacy; a sottoporre a verifiche di audit interno indipendenti l'attuazione dei piani di risposta e ripristino relativi alle TIC; a disporre di una funzione di gestione delle crisi; ad ampliare i test sulla continuità operativa e i piani di risposta e ripristino per descrivere gli scenari di passaggio tra le infrastrutture TIC primarie e quelle di ridondanza; a comunicare, su loro richiesta, alle autorità

([18]) 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).

competenti una stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC; a mantenere capacità di TIC ridondanti; a comunicare alle autorità nazionali competenti le modifiche apportate a seguito dei riesami successivi agli incidenti connessi alle TIC; a monitorare costantemente i pertinenti sviluppi tecnologici, a istituire un programma di test di resilienza operativa digitale esaustivo quale parte integrante del quadro per la gestione dei rischi informatici di cui al presente regolamento o ad adottare e riesaminare periodicamente una strategia per i rischi informatici derivanti da terzi. Inoltre, le microimprese dovrebbero essere tenute a valutare la necessità di mantenere tali capacità di TIC ridondanti solo sulla base del loro profilo di rischio. Le microimprese dovrebbero beneficiare di un regime più flessibile per quanto riguarda i programmi di test di resilienza operativa digitale. Quando valutano il tipo e la frequenza dei test da svolgere, dovrebbero trovare il giusto equilibrio tra l'obiettivo di mantenere un'elevata resilienza operativa digitale, le risorse disponibili e il loro profilo di rischio complessivo. Le microimprese e le entità finanziarie soggette al quadro semplificato per la gestione dei rischi informatici a norma al presente regolamento dovrebbero essere esentate dall'obbligo di svolgere test avanzati di strumenti, sistemi e processi di TIC fondati su test di penetrazione guidati dalla minaccia (*threat-led penetration testing* — TLPT), in quanto solo le entità finanziarie che soddisfano i criteri di cui al presente regolamento dovrebbero essere tenute a svolgere tali test. Alla luce delle loro limitate capacità, le microimprese dovrebbero poter concordare con il fornitore terzo di servizi TIC di delegare i diritti di accesso, ispezione e audit dell'entità finanziaria a un terzo indipendente nominato dal fornitore terzo di servizi TIC, a condizione che l'entità finanziaria possa richiedere in qualsiasi momento al rispettivo terzo indipendente tutte le informazioni e le garanzie pertinenti sulle prestazioni del fornitore terzo di servizi TIC.

(44) Dal momento che solo le entità finanziarie identificate ai fini dei test avanzati di resilienza digitale dovrebbero essere tenute a svolgere test di penetrazione basati su minacce, i processi amministrativi e i costi finanziari derivanti dallo svolgimento di tali test dovrebbero gravare soltanto su una piccola percentuale delle entità finanziarie.

(45) Per garantire il pieno allineamento e la coerenza complessiva tra le strategie aziendali delle entità finanziarie, da un lato, e la gestione dei rischi informatici, dall'altro, è opportuno richiedere agli organi di gestione delle entità finanziarie di mantenere un ruolo attivo e fondamentale nella guida e nell'adeguamento del quadro per la gestione dei rischi informatici e della strategia globale di resilienza operativa digitale. Gli organi di gestione dovrebbero adottare un approccio che non consideri solamente i mezzi per assicurare la resilienza dei sistemi di TIC, ma si estenda anche alle persone e ai processi mediante un ventaglio di strategie che promuovano, a ciascun livello dell'azienda e per tutto il personale, un forte senso di consapevolezza dei rischi informatici nonché l'impegno a osservare a tutti i livelli una rigorosa igiene informatica (*cyber hygiene*). La responsabilità principale dell'organo di gestione nell'affrontare i rischi informatici di un'entità finanziaria dovrebbe concretizzarsi nel principio guida di tale approccio complessivo, tradotto ulteriormente nel costante coinvolgimento dell'organo di gestione a controllare il monitoraggio della gestione dei rischi informatici.

(46) Inoltre, il principio della piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria si accompagna alla necessità di assicurare un livello di investimenti connessi alle TIC e un bilancio complessivo dell'entità finanziaria che consentirebbero all'entità finanziaria di conseguire un elevato livello di resilienza operativa digitale.

(47) Sulla scia delle migliori prassi, linee guida, raccomandazioni e approcci pertinenti a livello internazionale, nazionale e settoriale in materia di gestione dei rischi informatici, il presente regolamento promuove una serie di principi che favoriscono una struttura complessiva della gestione dei rischi informatici. Di conseguenza, nella misura in cui le principali capacità introdotte dalle entità finanziarie soddisfano le varie funzioni nella gestione dei rischi informatici (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione) indicate nel presente regolamento, le entità finanziarie dovrebbero conservare la libertà di impiegare modelli di gestione dei rischi informatici strutturati o categorizzati in maniera diversa.

(48) Per tenere il passo con l'evoluzione del contesto delle minacce informatiche, le entità finanziarie dovrebbero dotarsi di sistemi di TIC aggiornati, affidabili e capaci non solo per garantire il trattamento dei dati richiesto per i loro servizi, ma anche per assicurare una resilienza tecnologica sufficiente che consenta loro di fare adeguatamente fronte alle esigenze di trattamento aggiuntive derivanti da condizioni di stress del mercato o da altre situazioni avverse.

(49) È necessario adottare piani efficienti di continuità operativa e di ripristino che consentano alle entità finanziarie di risolvere tempestivamente e rapidamente gli incidenti connessi alle TIC, e in particolare gli attacchi informatici, limitando i danni e privilegiando la ripresa delle attività e le azioni di ripristino conformemente alle loro politiche di backup. Tuttavia, tale ripresa non dovrebbe in alcun modo mettere a repentaglio l'integrità e la sicurezza dei sistemi informatici e di rete, né la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati.

(50) Il presente regolamento permette alle entità finanziarie di fissare i loro obiettivi di tempo di ripristino e punto di ripristino (*recovery time and recovery point objectives*) in maniera flessibile e quindi di fissare tali obiettivi tenendo conto della natura e della criticità delle funzioni pertinenti nonché di eventuali esigenze aziendali specifiche, ma per fissare tali obiettivi dovrebbero comunque essere tenute a effettuare una valutazione del potenziale impatto sull'efficienza del mercato.

(51) I propagatori di attacchi informatici tendono a perseguire guadagni finanziari direttamente alla fonte, esponendo quindi le entità finanziarie a conseguenze significative. Per scongiurare il pericolo che i sistemi di TIC perdano l'integrità o divengano indisponibili e per evitare pertanto violazioni di dati e prevenire danni alle infrastrutture fisiche delle TIC, è opportuno migliorare e razionalizzare sensibilmente la segnalazione, da parte delle entità finanziarie, degli incidenti gravi connessi alle TIC. È opportuno armonizzare la segnalazione degli incidenti connessi alle TIC mediante l'introduzione di un obbligo per tutte le entità finanziarie di segnalare direttamente alle rispettive autorità competenti. Se un'entità finanziaria è soggetta alla vigilanza di più di un'autorità nazionale competente, gli Stati membri dovrebbero designare un'unica autorità competente quale destinataria di tale segnalazione. Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 del Consiglio ([19]) dovrebbero presentare tale segnalazione alle autorità nazionali competenti, che dovrebbero successivamente trasmettere la segnalazione alla Banca centrale europea (BCE).

(52) La segnalazione diretta dovrebbe consentire alle autorità di vigilanza finanziaria di avere immediato accesso alle informazioni relative agli incidenti gravi connessi alle TIC. Le autorità di vigilanza finanziaria dovrebbero a loro volta trasmettere i dettagli relativi agli incidenti gravi connessi alle TIC alle pubbliche autorità non finanziarie [quali le competenti autorità e i punti di contatto unici a norma della direttiva (UE) 2022/2555, le autorità nazionali per la protezione dei dati e le autorità di contrasto per gli incidenti gravi connessi alle TIC di natura penale], al fine di migliorare la consapevolezza di tali autorità in merito a tali incidenti e, nel caso dei CSIRT, di agevolare la tempestiva assistenza che può essere fornita alle entità finanziarie, se del caso. Gli Stati membri dovrebbero, inoltre, poter stabilire che le entità finanziarie stesse debbano fornire tali informazioni alle autorità pubbliche al di fuori del settore dei servizi finanziari. Tali flussi di informazioni dovrebbero consentire alle entità finanziarie di beneficiare rapidamente di qualsiasi contributo tecnico pertinente, di consulenza sui rimedi e del successivo seguito dato da tali autorità. Le informazioni sugli incidenti gravi connessi alle TIC dovrebbero essere oggetto di comunicazione reciproca: le autorità di vigilanza finanziaria dovrebbero fornire all'entità finanziaria tutti i riscontri o gli orientamenti necessari, mentre le AEV dovrebbero condividere, in forma anonima, le analisi delle minacce informatiche e le vulnerabilità concernenti un determinato incidente, per promuovere una più ampia difesa collettiva.

(53) Tutte le entità finanziarie dovrebbero essere tenute a effettuare segnalazioni di incidenti, ma tale obbligo non dovrebbe interessarle tutte allo stesso modo. Infatti, si dovrebbe procedere a una debita calibrazione delle soglie di rilevanza pertinenti, nonché delle tempistiche delle segnalazioni, nel contesto degli atti delegati basati sulle norme tecniche di regolamentazione che le AEV devono elaborare, al fine di cogliere unicamente gli incidenti gravi connessi alle TIC. Inoltre, le specificità delle entità finanziarie dovrebbero essere prese in considerazione nello stabilire il calendario per gli obblighi di segnalazione.

(54) Il presente regolamento dovrebbe imporre agli enti creditizi, agli istituti di pagamento, ai prestatori di servizi di informazione sui conti e agli istituti di moneta elettronica di segnalare tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti — precedentemente segnalati a norma della direttiva (UE) 2015/2366 — indipendentemente dalla natura TIC dell'incidente.

([19]) 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).

(55) Le AEV dovrebbero essere incaricate di valutare la fattibilità e le condizioni per una possibile centralizzazione delle segnalazioni di incidenti connessi alle TIC a livello dell'Unione. Tale centralizzazione potrebbe consistere in un unico polo dell'UE per la segnalazione di incidenti gravi connessi alle TIC che riceva direttamente le segnalazioni pertinenti e le notifichi automaticamente alle autorità nazionali competenti o che si limiti a centralizzare le segnalazioni pertinenti trasmesse dalle competenti autorità nazionali e pertanto assolva una funzione di coordinamento. Le AEV dovrebbero essere incaricate di preparare in collaborazione con la BCE e l'ENISA, una relazione comune che esamini la praticabilità dell'istituzione di un unico polo dell'UE.

(56) Per conseguire un elevato livello di resilienza operativa digitale, e in linea sia con le pertinenti norme internazionali (ad esempio, gli elementi fondamentali del G7 per i test di penetrazione basati su minacce) che con i quadri applicati nell'Unione, come TIBER-EU, le entità finanziarie dovrebbero sottoporre periodicamente a test i propri sistemi di TIC e il proprio personale con responsabilità connesse alle TIC per valutare l'efficacia delle relative capacità di prevenzione, individuazione, risposta e ripristino, allo scopo di scoprire e affrontare le potenziali vulnerabilità in materia di TIC. Per rispecchiare le differenze esistenti tra i vari sottosettori finanziari e all'interno di ognuno di essi per quanto riguarda il livello di preparazione delle entità finanziarie in materia di cibersicurezza, i test dovrebbero comprendere un'ampia varietà di strumenti e azioni, dalla valutazione dei requisiti di base (ad esempio valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle lacune, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente ove possibile, e test basati su scenari, test di compatibilità, test di prestazione o test end-to-end) fino a test più avanzati tramite TLPT. Tali test avanzati dovrebbero essere richiesti solo per le entità finanziarie che, nell'ambito delle TIC, hanno raggiunto la maturità sufficiente per svolgerli in modo ragionevole. I test di resilienza operativa digitale previsti dal presente regolamento dovrebbero essere pertanto più impegnativi per le entità finanziarie che soddisfano i criteri di cui al presente regolamento (ad esempio, enti creditizi grandi, sistemici e maturi a livello di TIC, le sedi di negoziazione, i depositari centrali di titoli e le controparti centrali ecc.) rispetto alle altre entità finanziarie. Allo stesso tempo i test di resilienza operativa digitale tramite TLPT dovrebbero essere più rilevanti per le entità finanziarie che operano in sottosettori chiave dei servizi finanziari e che assolvono una funzione sistemica (ad esempio pagamenti, attività bancaria, e compensazione e regolamento) e meno rilevanti per altri sottosettori (ad esempio gestori di patrimoni e agenzie di rating del credito).

(57) Le entità finanziarie coinvolte in attività transfrontaliere e che esercitano la libertà di stabilimento o la libera fornitura di servizi all'interno dell'Unione dovrebbero rispettare gli obblighi di un unico quadro di riferimento per i test avanzati (ossia i TLPT) nel proprio Stato membro di origine; tali test dovrebbero comprendere le infrastrutture delle TIC di tutte le giurisdizioni in cui il gruppo finanziario transfrontaliero opera all'interno dell'Unione, permettendo a tali gruppi finanziari transfrontalieri di sostenere i costi dei test connessi alle TIC in un'unica giurisdizione.

(58) Per avvalersi delle competenze già acquisite da talune autorità competenti, in particolare per quanto riguarda l'attuazione del quadro di riferimento TIBER-EU, il presente regolamento dovrebbe consentire agli Stati membri di designare un'autorità pubblica unica responsabile nel settore finanziario, a livello nazionale, per tutte le questioni relative ai TLPT, o alle autorità competenti, in assenza di tale designazione, di delegare l'esercizio dei compiti connessi ai TLPT a un'altra autorità finanziaria nazionale competente.

(59) Poiché il presente regolamento non impone alle entità finanziarie di coprire tutte le funzioni essenziali o importanti in un unico TLPT, le entità finanziarie dovrebbero essere libere di determinare quali e quante funzioni essenziali o importanti dovrebbero essere incluse nell'ambito di applicazione di tale test.

(60) I test congiunti ai sensi del presente regolamento - che comportano la partecipazione di diverse entità finanziarie a un TLPT e per cui un fornitore terzo di servizi TIC può direttamente stipulare accordi contrattuali con un soggetto incaricato dello svolgimento dei test esterno — dovrebbero essere ammessi solo qualora ci si attenda ragionevolmente che la qualità o la sicurezza dei servizi prestati dal fornitore terzo di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento, o la riservatezza dei dati relativi a tali servizi, subiscano ripercussioni negative. I test congiunti dovrebbero inoltre essere soggetti a garanzie (direzione da parte di un'entità finanziaria designata, calibrazione del numero di entità finanziarie partecipanti), al fine di assicurare un rigoroso esercizio di test per le entità finanziarie coinvolte che soddisfano gli obiettivi del TLPT conformemente al presente regolamento.

(61) Allo scopo di sfruttare le risorse interne disponibili a livello aziendale, il presente regolamento dovrebbe consentire il ricorso a soggetto incaricato dello svolgimento dei test interni ai fini dell'esecuzione del TLPT, a condizione che vi sia l'approvazione da parte delle autorità di vigilanza, che non vi sia alcun conflitto d'interessi e che vi sia un'alternanza periodica nel ricorso a soggetto incaricato dello svolgimento dei test interni ed esterni (ogni tre test), imponendo nel contempo che il fornitore di analisi delle minacce nel TLPT sia sempre esterno all'entità finanziaria. La responsabilità di condurre il TLPT dovrebbe rimanere interamente a carico dell'entità finanziaria. Le attestazioni fornite dalle autorità dovrebbero essere finalizzate esclusivamente al riconoscimento reciproco e non dovrebbero precludere eventuali azioni di follow-up necessarie per affrontare i rischi informatici a cui l'entità finanziaria è esposta, né dovrebbero essere considerati un avallo da parte delle autorità di vigilanza delle capacità di gestione e attenuazione dei rischi informatici di un'entità finanziaria.

(62) Per un solido monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario, è necessario stabilire una serie di norme basate su principi che guidino le entità finanziarie nel monitoraggio dei rischi che si presentano nel contesto di funzioni esternalizzate a fornitori terzi di servizi TIC, in particolare per i servizi TIC a supporto di funzioni essenziali o importanti, nonché più in generale nel contesto di tutte le dipendenze da terzi nel settore delle TIC.

(63) Per far fronte alla complessità delle varie fonti di rischi informatici, tenendo conto nel contempo della molteplicità e della diversità dei fornitori di soluzioni tecnologiche che consentono un'agevole fornitura di servizi finanziari, il presente regolamento dovrebbe applicarsi a un'ampia gamma di fornitori terzi di servizi TIC, compresi i fornitori di servizi di cloud computing, software, servizi di analisi dei dati e i fornitori di servizi di centri di elaborazione dati. Analogamente, poiché le entità finanziarie dovrebbero individuare e gestire in modo efficace e coerente tutti i tipi di rischio, anche nel contesto dei servizi TIC acquisiti all'interno di un gruppo finanziario, è opportuno chiarire che le imprese appartenenti a un gruppo finanziario e che forniscono servizi TIC prevalentemente alla loro impresa madre o a imprese figlie o succursali della loro impresa madre, nonché le entità finanziarie che forniscono servizi TIC ad altre entità finanziarie, dovrebbero essere considerate anch'esse fornitori terzi di servizi TIC ai sensi del presente regolamento. Infine, alla luce dell'evoluzione del mercato dei servizi di pagamento, sempre più dipendente da soluzioni tecniche complesse, e in vista delle tipologie emergenti di servizi di pagamento e di soluzioni connesse ai pagamenti, anche i partecipanti all'ecosistema dei servizi di pagamento, che prestano attività di trattamento dei pagamenti o gestiscono infrastrutture di pagamento, dovrebbero essere considerati fornitori terzi di servizi TIC ai sensi del presente regolamento, ad eccezione delle banche centrali quando gestiscono sistemi di pagamento o di regolamento titoli e delle autorità pubbliche quando forniscono servizi connessi alle TIC nel contesto dell'espletamento di funzioni di Stato.

(64) Un'entità finanziaria dovrebbe rimanere sempre responsabile del rispetto dei propri obblighi previsti dal presente regolamento. Le entità finanziarie dovrebbero svolgere il monitoraggio dei rischi emergenti a livello di fornitori terzi di servizi TIC secondo un approccio basato sulla proporzionalità, tenendo debitamente conto della natura, della portata, della complessità e della rilevanza delle loro dipendenza dai servizi TIC, della criticità o dell'importanza dei servizi, dei processi o delle funzioni oggetto degli accordi contrattuali e, in ultima analisi, sulla base di un'attenta valutazione di eventuali impatti sulla continuità e la qualità dei servizi finanziari a livello individuale e di gruppo, a seconda dei casi.

(65) Lo svolgimento di tale monitoraggio dovrebbe seguire un approccio strategico ai rischi informatici derivanti da terzi, formalizzato con l'adozione, da parte dell'organo di gestione dell'entità finanziaria, di una strategia dedicata per i rischi informatici derivanti da terzi fondata sul costante esame di tutte le dipendenze da terzi nel settore delle TIC. Affinché le autorità di vigilanza abbiano una visione più completa delle dipendenze da terzi nel settore delle TIC, e allo scopo di offrire ulteriore sostegno ai lavori nel contesto del quadro di sorveglianza istituito dal presente regolamento, tutte le entità finanziarie dovrebbero essere obbligate a tenere un registro delle informazioni contenente tutti gli accordi contrattuali sull'uso dei servizi TIC prestati da fornitori terzi di servizi TIC. Le autorità di vigilanza finanziaria dovrebbero avere la possibilità di richiedere il registro completo o chiedere sezioni specifiche dello stesso, ottenendo in tal modo informazioni essenziali per acquisire una più ampia comprensione delle dipendenze delle entità finanziarie in materia di TIC.

(66) Una meticolosa analisi precontrattuale dovrebbe precedere la conclusione formale degli accordi contrattuali e costituirne la base, in particolare concentrandosi su elementi quali la criticità o l'importanza dei servizi sostenuti dal contratto sulle TIC previsto, le necessarie approvazioni da parte delle autorità di vigilanza o altre condizioni, il possibile rischio di concentrazione che ne deriva, nonché applicando la dovuta diligenza nel processo di selezione e valutazione dei fornitori terzi di servizi TIC e valutando i potenziali conflitti d'interessi. Per gli accordi contrattuali riguardanti funzioni essenziali o importanti, le entità finanziarie dovrebbero prendere in considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli standard più aggiornati ed elevati in materia di sicurezza delle informazioni. La risoluzione degli accordi contrattuali potrebbe giustificarsi almeno sulla base di una serie di

circostanze che attestino carenze addebitabili al fornitore terzo di servizi TIC, in particolare rilevanti violazioni di leggi o condizioni contrattuali, circostanze che rivelano una potenziale alterazione dell'esercizio delle funzioni previste negli accordi contrattuali, punti deboli del fornitore terzo di servizi TIC emersi nella sua gestione complessiva dei rischi informatici o circostanze che indicano l'inabilità dell'autorità competente interessata di vigilare efficacemente sull'entità finanziaria.

(67) Per far fronte all'impatto sistemico del rischio di concentrazione di servizi TIC forniti da terzi, il presente regolamento promuove una soluzione equilibrata tramite l'assunzione di un approccio flessibile e graduale verso tale rischio di concentrazione, in quanto l'imposizione di massimali rigidi o restrizioni rigorose potrebbe intralciare lo svolgimento dell'attività economica e limitare la libertà contrattuale. Le entità finanziarie dovrebbero valutare meticolosamente le disposizioni contrattuali previste per verificare la probabilità che tali rischi si presentino, anche mediante analisi approfondite degli accordi di subappalto, soprattutto quando siano conclusi con fornitori terzi di servizi TIC stabiliti in un paese terzo. In questa fase, e allo scopo di trovare il giusto equilibrio tra l'imperativo di preservare la libertà contrattuale e quello di garantire la stabilità finanziaria, non si considera opportuno prevedere norme su massimali e limiti rigorosi alle esposizioni verso terzi nel settore delle TIC. Nel contesto del quadro di sorveglianza, un'autorità di sorveglianza capofila nominata ai sensi del presente regolamento, dovrebbe, rispetto a fornitori terzi critici di servizi TIC, accertarsi con particolare cura di comprendere a fondo le dimensioni delle interdipendenze, di scoprire i casi specifici in cui un elevato grado di concentrazione di fornitori terzi critici di servizi TIC nell'Unione potrebbe compromettere l'integrità e la stabilità del sistema finanziario dell'Unione e di mantenere un dialogo con i fornitori terzi critici di servizi TIC laddove tale rischio specifico sia identificato.

(68) Per valutare e monitorare costantemente la capacità del fornitore terzo di servizi TIC di erogare in sicurezza i servizi all'entità finanziaria senza effetti avversi sulla resilienza operativa digitale di quest'ultima, è opportuno armonizzare diversi elementi contrattuali chiave con i fornitori terzi di servizi TIC. Tale armonizzazione dovrebbe coprire gli ambiti minimi che sono cruciali per consentire un monitoraggio completo, da parte dell'entità finanziaria, dei rischi che potrebbero derivare dal fornitore terzo di servizi TIC, nella prospettiva dell'esigenza dell'entità finanziaria di garantire la propria resilienza digitale, poiché dipendente in larga misura dalla stabilità, dalla funzionalità, dalla disponibilità e dalla sicurezza dei servizi TIC ricevuti.

(69) In sede di rinegoziazione degli accordi contrattuali al fine di perseguire la conformità con i requisiti del presente regolamento, le entità finanziarie e i fornitori terzi di servizi TIC dovrebbero garantire la copertura delle principali disposizioni contrattuali di cui al presente regolamento.

(70) La definizione di «funzione essenziale o importante» di cui al presente regolamento comprende le «funzioni essenziali» definite all'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE del Parlamento europeo e del Consiglio ([20]). Di conseguenza, le funzioni ritenute essenziali ai sensi della direttiva 2014/59/UE sono incluse nella definizione di funzioni essenziali ai sensi del presente regolamento.

(71) Indipendentemente dall'essenzialità o dall'importanza della funzione supportata dai servizi TIC, gli accordi contrattuali dovrebbero, in particolare, contenere le descrizioni complete di funzioni e servizi, l'indicazione delle località in cui si esercitano tali funzioni e deve aver luogo il trattamento dei dati nonché le descrizioni dei livelli di servizio. Altri elementi essenziali per consentire il monitoraggio, da parte di un'entità finanziaria, dei rischi informatici derivanti da terzi sono: disposizioni contrattuali che specificano in che modo il fornitore terzo di servizi TIC garantisce l'accessibilità, la disponibilità, l'integrità, la sicurezza e la protezione dei dati personali; disposizioni che stabiliscono le pertinenti garanzie per consentire l'accesso, il ripristino e la restituzione dei dati in caso di insolvenza, risoluzione o cessazione dell'operatività del fornitore terzo di servizi TIC, nonché disposizioni che impongono al fornitore terzo di servizi TIC di prestare assistenza in caso di incidenti connessi alle TIC in relazione ai servizi forniti, senza costi supplementari oppure a un costo stabilito ex ante; disposizioni sull'obbligo per il

([20]) 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).

fornitore terzo di servizi TIC di cooperare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria; e disposizioni sui diritti di risoluzione e sui relativi termini minimi di preavviso per la risoluzione degli accordi contrattuali, conformemente alle attese delle autorità competenti e delle autorità di risoluzione.

(72) In aggiunta a tali disposizioni contrattuali e al fine di garantire che le entità finanziarie mantengano il pieno controllo di tutti gli sviluppi a livello di soggetti terzi che potrebbero comprometterne la sicurezza delle TIC, i contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti dovrebbero altresì prevedere quanto segue: le descrizioni complete dei livelli di servizio, con precisi obiettivi quantitativi e qualitativi, in termini di prestazioni, in modo da consentire l'applicazione, senza indebito ritardo, di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati; i pertinenti termini di preavviso e obblighi di segnalazione per il fornitore terzo di servizi TIC nel caso di sviluppi che possano incidere seriamente sulla capacità di tale fornitore di fornire efficacemente i rispettivi servizi TIC; l'obbligo per il fornitore terzo di servizi TIC di attuare e testare i piani operativi d'emergenza e di disporre di misure, strumenti e politiche per la sicurezza delle TIC che consentano la fornitura sicura dei servizi, nonché di partecipare e di cooperare pienamente al TLPT svolto dall'entità finanziaria.

(73) I contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti dovrebbero altresì contenere disposizioni che consentano i diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un soggetto terzo designato, nonché il diritto di ottenere copia, quali strumenti fondamentali per il monitoraggio costante, da parte delle entità finanziarie, delle prestazioni del fornitore terzo di servizi TIC, insieme alla piena collaborazione di quest'ultimo nel corso delle ispezioni. Analogamente, l'autorità competente dell'entità finanziaria dovrebbe poter godere del diritto, sulla base di preavvisi, di ispezionare e sottoporre a verifiche di audit il fornitore terzo di servizi TIC, fatta salva la protezione delle informazioni riservate.

(74) Tali accordi contrattuali dovrebbero inoltre prevedere strategie di uscita dedicate che consentano in particolare periodi di transizione obbligatori durante i quali i fornitori terzi di servizi TIC dovrebbero continuare a prestare i pertinenti servizi, allo scopo di ridurre il rischio di perturbazioni a livello dell'entità finanziaria o di consentire a quest'ultima di passare senza inconvenienti all'utilizzo di altri fornitori terzi di servizi TIC o, in alternativa, di adottare soluzioni interne, in funzione della complessità del servizio TIC fornito. Inoltre, le entità finanziarie che rientrano nell'ambito di applicazione della direttiva 2014/59/UE dovrebbero garantire che i pertinenti contratti per i servizi TIC siano solidi e pienamente applicabili in caso di risoluzione di tali entità finanziarie. In linea con le aspettative delle autorità di risoluzione, tali entità finanziarie dovrebbero pertanto garantire che i pertinenti contratti di servizi TIC siano resilienti in caso di risoluzione. Finché continuano a rispettare i loro obblighi di pagamento, tali entità finanziarie dovrebbero garantire, tra gli altri requisiti, che i pertinenti contratti per i servizi TIC contengano clausole di non risoluzione, di non sospensione e di immodificabilità in caso di ristrutturazione o risoluzione.

(75) Inoltre, l'utilizzo volontario di clausole contrattuali standard elaborate da autorità pubbliche o istituzioni dell'Unione, in particolare l'utilizzo di clausole contrattuali elaborate dalla Commissione per i servizi di cloud computing, potrebbe costituire un'ulteriore preziosa risorsa per le entità finanziarie e per i fornitori terzi di servizi TIC, accrescendo il loro livello di certezza del diritto in merito all'utilizzo di servizi di cloud computing nel settore finanziario, in completa conformità con i requisiti e le aspettative definiti dalla normativa dell'Unione in materia di servizi finanziari. L'elaborazione di clausole contrattuali standard si fonda su misure già previste dal piano d'azione per le tecnologie finanziarie del 2018, in cui la Commissione annunciava l'intenzione di incoraggiare e agevolare lo sviluppo di clausole contrattuali standard per l'esternalizzazione di servizi di cloud computing da parte delle entità finanziarie, basandosi sulle iniziative intersettoriali già intraprese dai portatori di interessi del settore dei servizi di cloud computing che la Commissione ha favorito grazie al coinvolgimento del settore finanziario.

(76) Per promuovere la convergenza e l'efficienza negli approcci di vigilanza quando si affrontano rischi relativi alle TIC derivanti da terzi nel settore finanziario, nonché per rafforzare la resilienza operativa digitale delle entità finanziarie che dipendono da fornitori terzi critici di servizi TIC per la fornitura di servizi TIC che sostengono la fornitura dei servizi finanziari e contribuire così a preservare la stabilità del sistema finanziario dell'Unione e l'integrità del mercato interno per i servizi finanziari, è opportuno assoggettare i fornitori terzi critici di servizi TIC a un quadro di sorveglianza dell'Unione. Sebbene l'istituzione del quadro di sorveglianza sia giustificata dal valore aggiunto di un'azione intrapresa a livello dell'Unione e in virtù del ruolo intrinseco e delle specificità dell'utilizzo dei servizi TIC

nella fornitura di servizi finanziari, è opportuno ricordare, nel contempo, che tale soluzione appare adeguata solo nel contesto del presente regolamento, che tratta specificamente della resilienza operativa digitale nel settore finanziario. Tuttavia, tale quadro di sorveglianza non dovrebbe essere considerato un nuovo modello di vigilanza dell'Unione in altri settori delle attività e dei servizi finanziari.

(77) Il quadro di sorveglianza dovrebbe applicarsi solo ai fornitori terzi critici di servizi TIC. Dovrebbe pertanto esserci un meccanismo di designazione, in modo da tenere conto della dimensione e della natura della dipendenza del settore finanziario da tali fornitori terzi di servizi TIC. Tale meccanismo dovrebbe comportare una serie di criteri quantitativi e qualitativi per fissare i parametri di criticità come base per l'inclusione nel quadro di sorveglianza. Al fine di garantire l'accuratezza di tale valutazione, e indipendentemente dalla struttura aziendale del fornitore terzo di servizi TIC, tali criteri, nel caso di un fornitore terzo di servizi TIC appartenente a un gruppo più ampio, dovrebbero prendere in considerazione l'intera struttura del gruppo del fornitore terzo di servizi TIC. Da un lato, i fornitori terzi critici di servizi TIC, che non sono designati automaticamente in virtù dell'applicazione di tali criteri, dovrebbero avere la possibilità di aderire al quadro di sorveglianza su base volontaria; dall'altro, i fornitori terzi di servizi TIC, che sono già soggetti ai quadri dei meccanismi di sorveglianza che sostengono l'assolvimento dei compiti del Sistema europeo di banche centrali di cui all'articolo 127, paragrafo 2, TFUE, dovrebbero esserne esentati.

(78) Analogamente, anche le entità finanziarie che forniscono servizi TIC ad altre entità finanziarie, pur appartenendo alla categoria dei fornitori terzi di servizi TIC ai sensi del presente regolamento, dovrebbero essere esentate dal quadro di sorveglianza in quanto già soggette ai meccanismi di vigilanza istituiti dalla pertinente normativa dell'Unione in materia di servizi finanziari. Ove applicabile, le autorità competenti dovrebbero tenere conto, nell'ambito delle loro attività di vigilanza, dei rischi informatici posti alle entità finanziarie dalle entità finanziarie che forniscono servizi TIC. Allo stesso modo, a causa degli attuali meccanismi di monitoraggio dei rischi a livello di gruppo, la stessa esenzione dovrebbe essere introdotta per i fornitori terzi di servizi TIC che prestano servizi prevalentemente alle entità del loro stesso gruppo. Anche i fornitori terzi di servizi TIC che prestano servizi TIC unicamente in uno Stato membro a entità finanziarie attive solo in tale Stato membro dovrebbero essere esentati dal meccanismo di designazione a causa delle loro attività limitate e della mancanza di impatto transfrontaliero.

(79) La trasformazione digitale che interessa i servizi finanziari ha portato a un livello senza precedenti di utilizzo dei servizi TIC e di dipendenza da essi. Poiché è divenuto inconcepibile fornire servizi finanziari senza l'utilizzo di servizi di cloud computing, soluzioni software e servizi connessi ai dati, l'ecosistema finanziario dell'Unione è diventato intrinsecamente codipendente da taluni servizi TIC prestati dai fornitori di servizi TIC. Alcuni di questi fornitori, innovatori nello sviluppo e nell'applicazione di tecnologie basate sulle TIC, svolgono un ruolo significativo nella fornitura di servizi finanziari, o sono diventati parte integrante della catena del valore dei servizi finanziari. Sono quindi divenuti fondamentali per la stabilità e l'integrità del sistema finanziario dell'Unione. Questa diffusa dipendenza dai servizi prestati da fornitori terzi critici di servizi TIC, unitamente all'interdipendenza dei sistemi informativi di vari operatori di mercato, crea un rischio diretto, e potenzialmente grave, per il sistema dei servizi finanziari dell'Unione e per la continuità della fornitura di servizi finanziari, qualora i fornitori terzi critici di servizi TIC fossero colpiti da perturbazioni operative o gravi incidenti informatici. Gli incidenti informatici hanno la capacità distintiva di moltiplicarsi e propagarsi in tutto il sistema finanziario a un ritmo notevolmente più rapido rispetto ad altri tipi di rischi monitorati nel settore finanziario e possono estendersi a tutti i settori e oltre i confini geografici. Sono potenzialmente in grado di evolvere verso una crisi sistemica, in cui la fiducia nel sistema finanziario si è erosa a causa dell'interruzione delle funzioni che sostengono l'economia reale, o di ingenti perdite finanziarie, raggiungendo un livello che il sistema finanziario non è in grado di sopportare, o che richiede la messa a punto di pesanti misure di assorbimento degli shock. Per evitare che tali scenari si verifichino e compromettano in tal modo la stabilità finanziaria e l'integrità dell'Unione, è essenziale assicurare la convergenza delle pratiche di vigilanza connesse ai rischi informatici derivanti da terzi nella finanza, in particolare attraverso nuove norme che consentano la sorveglianza da parte dell'Unione dei fornitori terzi critici di servizi TIC.

(80) Il quadro di sorveglianza dipende in larga misura dal grado di collaborazione tra l'autorità di sorveglianza capofila e il fornitore terzo critico di servizi TIC che presta alle entità finanziarie servizi che incidono sulla fornitura di servizi finanziari. Una sorveglianza efficace si basa, tra l'altro, sulla capacità dell'autorità di sorveglianza capofila di svolgere efficacemente missioni di monitoraggio e ispezioni per valutare le norme, i controlli e i processi utilizzati dai fornitori terzi critici di servizi TIC, nonché per valutare il potenziale impatto cumulativo delle loro attività sulla stabilità finanziaria e sull'integrità del sistema finanziario. Allo stesso tempo, è fondamentale che i fornitori terzi critici di servizi TIC seguano le raccomandazioni dell'autorità di sorveglianza capofila e rispondano alle sue preoccupazioni. Poiché la mancanza di cooperazione da parte di un fornitore terzo di servizi TIC critico che fornisce servizi che incidono sulla fornitura di servizi finanziari, come il rifiuto di concedere l'accesso ai propri locali o di trasmettere informazioni, priverebbe in ultima analisi l'autorità di sorveglianza capofila dei suoi strumenti essenziali per valutare i rischi informatici derivanti da terzi e potrebbe incidere negativamente sulla stabilità finanziaria e sull'integrità del sistema finanziario, occorre prevedere anche un regime sanzionatorio commisurato.

(81) In tale contesto, la necessità dell'autorità di sorveglianza capofila di imporre penalità di mora per obbligare i fornitori terzi critici di servizi TIC a rispettare gli obblighi in materia di trasparenza e accesso di cui al presente regolamento non dovrebbe essere messa a repentaglio dalle difficoltà derivanti dall'applicazione di tali penalità di mora in relazione a fornitori terzi critici di servizi TIC stabiliti in paesi terzi. Al fine di garantire l'applicabilità di tali penalità e consentire una rapida introduzione delle procedure a tutela dei diritti della difesa dei fornitori terzi critici di servizi TIC nel contesto del meccanismo di designazione e della formulazione di raccomandazioni, tali fornitori terzi critici di servizi TIC che forniscono alle entità finanziarie servizi che incidono sulla fornitura di servizi finanziari dovrebbero essere tenuti a mantenere un'adeguata presenza commerciale nell'Unione. Data la natura della sorveglianza e l'assenza di accordi comparabili in altre giurisdizioni, non esistono meccanismi alternativi adeguati che garantiscano tale obiettivo mediante una cooperazione efficace con le autorità di vigilanza finanziaria nei paesi terzi in relazione al monitoraggio dell'impatto dei rischi operativi digitali posti dai fornitori terzi di servizi TIC sistemici, che rientrano nella designazione di fornitori terzi critici di servizi TIC stabiliti in paesi terzi. Pertanto, onde continuare a fornire servizi TIC a entità finanziarie nell'Unione, un fornitore terzo di servizi TIC stabilito in un paese terzo che sia stato designato come critico a norma del presente regolamento dovrebbe stipulare, entro 12 mesi da tale designazione, tutti gli accordi necessari per garantire la propria integrazione nell'Unione, mediante l'istituzione di un'impresa figlia, quale definita nell'acquis dell'Unione, segnatamente nella direttiva 2013/34/UE del Parlamento europeo e del Consiglio ([21]).

(82) L'obbligo di istituire un'impresa figlia nell'Unione non dovrebbe impedire al fornitore terzo critico di servizi TIC di prestare servizi TIC e il relativo sostegno tecnico da impianti e infrastrutture situati al di fuori dell'Unione. Il presente regolamento non impone un obbligo di localizzazione dei dati poiché non impone di conservare o trattare i dati nell'Unione.

(83) I fornitori terzi critici di servizi TIC dovrebbero essere in grado di fornire servizi TIC da ovunque nel mondo, non necessariamente o non solo da locali situati nell'Unione. Le attività di sorveglianza dovrebbero essere svolte in primo luogo in locali situati nell'Unione e interagendo con soggetti situati nell'Unione, comprese le imprese figlie istituite da fornitori terzi critici di servizi TIC a norma del presente regolamento. Tuttavia, tali azioni all'interno dell'Unione potrebbero essere insufficienti per consentire all'autorità di sorveglianza capofila di svolgere pienamente ed efficacemente i propri compiti ai sensi del presente regolamento. L'autorità di sorveglianza capofila dovrebbe pertanto essere in grado di esercitare i pertinenti poteri di sorveglianza anche nei paesi terzi. L'esercizio di tali poteri nei paesi terzi dovrebbe consentire all'autorità di sorveglianza capofila di esaminare le strutture dalle quali i servizi TIC o di assistenza tecnica sono effettivamente forniti o gestiti dal fornitore terzo critico di servizi TIC, e dovrebbe fornire all'autorità di sorveglianza capofila una comprensione completa e operativa della gestione dei rischi informatici da parte del fornitore terzo critico di servizi TIC. La possibilità per l'autorità di sorveglianza capofila, in quanto agenzia dell'Unione, di esercitare poteri al di fuori del territorio dell'Unione dovrebbe essere debitamente inquadrata da condizioni pertinenti, in particolare il consenso del fornitore terzo critico di servizi TIC interessato. Analogamente, le autorità pertinenti del paese terzo dovrebbero essere informate dell'esercizio nel proprio territorio delle attività dell'autorità di sorveglianza capofila e non esservisi opposte. Tuttavia, al fine di garantire un'attuazione efficace e fatte salve le rispettive competenze delle istituzioni dell'Unione e degli Stati membri, tali poteri devono

([21]) Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE del Consiglio (GU L 182 del 29.6.2013, pag. 19).

altresì essere pienamente basati sulla conclusione di accordi di cooperazione amministrativa con le autorità pertinenti del paese terzo interessato. Il presente regolamento dovrebbe pertanto consentire alle AEV di concludere accordi di cooperazione amministrativa con le autorità pertinenti dei paesi terzi, che non dovrebbero altrimenti generare obblighi giuridici in capo all'Unione e ai suoi Stati membri.

(84) Per facilitare la comunicazione con l'autorità di sorveglianza capofila e garantire un'adeguata rappresentanza, i fornitori terzi critici di servizi TIC che fanno parte di un gruppo dovrebbero designare una persona giuridica come punto di coordinamento.

(85) Il quadro di sorveglianza non dovrebbe pregiudicare la competenza degli Stati membri per quanto attiene allo svolgimento di proprie missioni di sorveglianza o di monitoraggio nei confronti di fornitori terzi di servizi TIC che non sono designati come critici ai sensi del presente regolamento ma sono considerati importanti a livello nazionale.

(86) Per sfruttare l'architettura istituzionale del settore dei servizi finanziari, articolata su vari livelli, il comitato congiunto delle AEV dovrebbe continuare a garantire il coordinamento intersettoriale complessivo su tutte le questioni concernenti i rischi informatici, conformemente ai propri compiti in materia di cibersicurezza. Dovrebbe essere coadiuvato da un nuovo sottocomitato (forum di sorveglianza) che dovrebbe svolgere il lavoro preparatorio, sia per le singole decisioni rivolte a fornitori terzi critici di servizi TIC, sia per la formulazione di raccomandazioni collettive, relative in particolare all'analisi comparativa dei programmi di sorveglianza per i fornitori terzi critici di servizi TIC, nonché all'identificazione delle migliori prassi riguardanti il rischio di concentrazione delle TIC.

(87) Per far sì che i fornitori terzi critici di servizi TIC siano soggetti a una sorveglianza adeguata ed efficace a livello dell'Unione, il presente regolamento prevede che una qualunque delle tre AEV possa essere designata come autorità di sorveglianza capofila. L'assegnazione individuale di un fornitore terzo critico di servizi TIC a una delle tre AEV dovrebbe essere fondata su una valutazione della prevalenza delle entità finanziarie che operano nei settori finanziari per i quali tale AEV è competente. Tale approccio dovrebbe portare a una ripartizione equilibrata dei compiti e delle responsabilità tra le tre AEV, nel contesto dell'esercizio delle funzioni di sorveglianza, e dovrebbe utilizzare al meglio le risorse umane e le competenze tecniche disponibili in ciascuna delle tre AEV.

(88) Alle autorità di sorveglianza capofila dovrebbero essere attribuiti i poteri necessari per condurre indagini, effettuare ispezioni in fuori sede o presso i locali e le sedi dei fornitori terzi critici di servizi TIC e ottenere informazioni complete e aggiornate. Tali poteri dovrebbero consentire all'autorità di sorveglianza capofila di acquisire un'immagine realistica del tipo, delle dimensioni e dell'impatto dei rischi informatici derivanti da terzi cui sono esposte le entità finanziarie e, in ultima analisi, il sistema finanziario dell'Unione. Affidare alle AEV il ruolo di sorveglianza principale è un prerequisito per comprendere e affrontare la dimensione sistemica dei rischi informatici nel settore finanziario. L'impatto dei fornitori terzi critici di servizi TIC sul settore finanziario dell'Unione e i problemi causati dal rischio di concentrazione delle TIC che ne possono derivare esigono un approccio collettivo a livello dell'UE. L'esecuzione contestuale di molteplici audit e diritti di accesso, effettuata separatamente da varie autorità competenti, con un coordinamento scarso o nullo tra di esse, impedirebbe alle autorità di vigilanza finanziaria di ottenere un quadro completo ed esaustivo dei rischi informatici derivanti da terzi nell'Unione, e provocherebbe anzi sovrapposizioni, oneri e complessità per i fornitori terzi critici di servizi TIC qualora fossero soggetti a un gran numero di richieste di monitoraggio e ispezione.

(89) A causa dell'impatto significativo del fatto di essere designati come critici, il presente regolamento dovrebbe garantire che i diritti dei fornitori terzi critici di servizi TIC siano preservati in tutte le fasi di attuazione del quadro di sorveglianza. Prima di essere designati come critici, tali fornitori dovrebbero, ad esempio, avere il diritto di presentare all'autorità di sorveglianza capofila una dichiarazione motivata contenente tutte le informazioni pertinenti ai fini della valutazione relativa alla loro designazione. Dal momento che all'autorità di sorveglianza capofila dovrebbe essere conferito il potere di presentare raccomandazioni su questioni concernenti i rischi informatici e sui rimedi idonei, ivi compreso il potere di opporsi a determinate disposizioni contrattuali suscettibili in ultima analisi di incidere sulla stabilità dell'entità finanziaria o del sistema finanziario, prima di finalizzare tali raccomandazioni i fornitori terzi critici di servizi TIC dovrebbero altresì avere l'opportunità di fornire spiegazioni riguardo all'impatto previsto delle soluzioni, proposte nelle raccomandazioni, sui clienti che sono entità non

rientranti nell'ambito di applicazione del presente regolamento, formulando soluzioni per attenuare i rischi. I fornitori terzi critici di servizi TIC in disaccordo con le raccomandazioni dovrebbero presentare una spiegazione motivata della loro intenzione di non uniformarsi alla raccomandazione. Se tale spiegazione motivata non è presentata o è ritenuta insufficiente, l'autorità di sorveglianza capofila dovrebbe pubblicare un avviso pubblico che descriva sommariamente la questione dell'inosservanza.

(90) Nell'ambito delle loro funzioni relative alla vigilanza prudenziale delle entità finanziarie, le autorità competenti dovrebbero debitamente includere il compito di verificare il rispetto sostanziale delle raccomandazioni formulate dall'autorità di sorveglianza capofila. Le autorità competenti dovrebbero poter imporre alle entità finanziarie di adottare misure supplementari per affrontare i rischi individuati nelle raccomandazioni dell'autorità di sorveglianza capofila e dovrebbero, a tempo debito, pubblicare notifiche a tal fine. Se l'autorità di sorveglianza capofila rivolge raccomandazioni ai fornitori terzi critici di servizi TIC sottoposti a vigilanza ai sensi della direttiva (UE) 2022/2555, le autorità competenti dovrebbero poter consultare, su base volontaria e prima di adottare misure supplementari, le autorità competenti ai sensi di tale direttiva per promuovere un approccio coordinato nei confronti dei fornitori terzi critici di servizi TIC in questione.

(91) L'esercizio della sorveglianza dovrebbe essere guidato da tre principi operativi volti a garantire: a) uno stretto coordinamento tra le AEV nel loro ruolo di autorità di sorveglianza capofila, attraverso una rete di sorveglianza comune, b) la coerenza con il quadro istituito dalla direttiva (UE) 2022/2555 (attraverso una consultazione volontaria degli organismi ai sensi di tale direttiva per evitare la duplicazione di misure rivolte ai fornitori terzi critici di servizi TIC), e c) l'applicazione della diligenza per ridurre al minimo il rischio potenziale di perturbazione dei servizi forniti dai fornitori terzi critici di servizi TIC ai clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento.

(92) Il quadro di sorveglianza non dovrebbe rimpiazzare, né in alcun modo o in alcuna parte sostituirsi, alla prescrizione relativa alla gestione, da parte delle entità finanziarie, dei rischi derivanti dal ricorso a fornitori terzi di servizi TIC, compreso l'obbligo di mantenere un monitoraggio costante degli accordi contrattuali stipulati con fornitori terzi critici di servizi TIC. Analogamente, il quadro di sorveglianza non dovrebbe incidere sulla piena responsabilità delle entità finanziarie per quanto riguarda il rispetto e l'adempimento di tutti gli obblighi di legge previsti dal presente regolamento e dalla pertinente normativa in materia di servizi finanziari.

(93) Per evitare duplicazioni e sovrapposizioni, è opportuno che le autorità competenti si astengano dall'adozione individuale di misure per il monitoraggio dei rischi derivanti da fornitori terzi critici di servizi TIC; a tale riguardo, esse dovrebbero affidarsi alla pertinente valutazione dell'autorità di sorveglianza capofila. Eventuali misure dovrebbero in ogni caso essere coordinate e concordate preliminarmente con l'autorità di sorveglianza capofila nel contesto dell'esercizio dei compiti del quadro di sorveglianza.

(94) Per promuovere la convergenza a livello internazionale sull'utilizzo delle migliori prassi per il riesame e il monitoraggio della gestione del rischio digitale derivante da fornitori terzi di servizi TIC, è opportuno incoraggiare le AEV a stipulare accordi di cooperazione con le pertinenti autorità normative e di vigilanza di paesi terzi.

(95) Per sfruttare utilmente le competenze specifiche, le capacità tecniche e l'esperienza del personale specializzato nella gestione dei rischi operativi e informatici all'interno delle autorità competenti, le tre AEV e, su base volontaria, le autorità competenti ai sensi della direttiva (UE) 2022/2555 e l'autorità di sorveglianza capofila dovrebbero tener conto delle capacità e conoscenze delle autorità di vigilanza nazionali e istituire gruppi destinati a esaminare i singoli fornitori terzi critici di servizi TIC, riunendo gruppi multidisciplinari che coadiuvino la preparazione e l'attuazione delle attività di sorveglianza, comprese le indagini generali e le ispezioni dei fornitori terzi critici di servizi TIC, nonché l'eventuale seguito necessario da dare a queste attività.

(96) Mentre i costi derivanti dai compiti di sorveglianza sarebbero interamente finanziati dalle commissioni applicate ai fornitori terzi critici di servizi TIC, è tuttavia probabile che le AEV debbano sostenere, prima dell'avvio del quadro di sorveglianza, costi per l'attuazione di sistemi di TIC dedicati a sostegno dell'imminente sorveglianza, poiché sarebbe necessario sviluppare e attivare in anticipo sistemi di TIC dedicati. Il presente regolamento prevede pertanto un modello di finanziamento ibrido, in base al quale il quadro di sorveglianza sarebbe, in quanto tale, interamente finanziato tramite commissioni, mentre lo sviluppo dei sistemi di TIC delle AEV sarebbe finanziato dai contributi dell'Unione e delle autorità nazionali competenti.

(97) Al fine di garantire il corretto esercizio dei propri compiti ai sensi del presente regolamento, le autorità competenti dovrebbero detenere tutti i necessari poteri per vigilare, indagare e imporre sanzioni. Esse dovrebbero, in linea di principio, pubblicare avvisi relativi alle sanzioni amministrative che irrogano. Poiché è possibile che entità finanziarie e fornitori terzi di servizi TIC siano stabiliti in Stati membri diversi e siano sottoposti a vigilanza da parte di differenti autorità competenti, è opportuno che l'applicazione del presente regolamento sia agevolata, da una parte, attraverso una stretta cooperazione tra le autorità competenti interessate, compresa la BCE per quanto riguarda i compiti specifici a essa attribuiti dal regolamento (UE) n. 1024/2013 del Consiglio, e, dall'altra, mediante consultazioni con le AEV tramite il reciproco scambio di informazioni e l'offerta di assistenza nel contesto delle attività di vigilanza pertinenti.

(98) Per quantificare e qualificare ulteriormente i criteri per la designazione di fornitori terzi di servizi TIC come critici e per armonizzare le commissioni per le attività di sorveglianza, è opportuno delegare alla Commissione il potere di adottare atti ai sensi dell'articolo 290 TFUE al fine di integrare il presente regolamento precisando ulteriormente l'impatto sistemico che un guasto o un'indisponibilità operativa presso un fornitore terzo di servizi TIC potrebbe esercitare sulle entità finanziarie cui fornisce servizi TIC, il numero di enti a rilevanza sistemica a livello globale (*global systemically important institutions* — G-SII) o di altri enti a rilevanza sistemica (*other systemically important institutions* — O-SII) che dipendono dal rispettivo fornitore terzo di servizi TIC, il numero di fornitori terzi di servizi TIC attivi su uno specifico mercato, i costi della migrazione di dati e di carichi di lavoro relativi alle TIC ad altri fornitori terzi di servizi TIC, nonché l'importo delle commissioni per le attività di sorveglianza e le relative modalità di pagamento. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, e che tali consultazioni siano condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([22]). In particolare, al fine di garantire la partecipazione su un piede di parità alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(99) Le norme tecniche di regolamentazione dovrebbero garantire la coerente armonizzazione i requisiti contenuti nel presente regolamento. Nel loro ruolo di organismi con una competenza altamente specializzata, le AEV dovrebbero elaborare progetti di norme tecniche di regolamentazione che non comportino scelte politiche e presentarli alla Commissione. È opportuno elaborare norme tecniche di regolamentazione nei settori della gestione dei rischi informatici, della segnalazione di incidenti gravi connessi alle TIC e dei test, nonché per quanto riguarda i requisiti principali per un solido monitoraggio dei rischi informatici derivanti da terzi. La Commissione e le AEV dovrebbero fare in modo che tutte le entità finanziarie possano applicare tali norme e requisiti in misura proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, delle loro attività e della loro operatività. Alla Commissione si dovrebbe conferire il potere di adottare tali norme tecniche di regolamentazione mediante atti delegati a norma dell'articolo 290 TFUE e degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

(100) Per rendere più agevolmente comparabili le segnalazioni sugli incidenti gravi connessi alle TIC e sui gravi incidenti operativi o relativi alla sicurezza dei pagamenti, nonché per garantire la trasparenza sugli accordi contrattuali per l'utilizzo di servizi TIC offerti da fornitori terzi, le AEV dovrebbero elaborare progetti di norme tecniche di attuazione che introducano modelli, formulari e procedure standardizzati per la segnalazione, da parte delle entità finanziarie, degli incidenti gravi connessi alle TIC e di gravi incidenti operativi o relativi alla sicurezza dei pagamenti, nonché modelli standardizzati per il registro delle informazioni. Al momento di elaborare tali norme, le AEV dovrebbero tenere conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni. È opportuno conferire alla Commissione il potere di adottare tali norme tecniche di attuazione mediante atti di esecuzione a norma dell'articolo 291 TFUE e dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

([22]) GU L 123 del 12.5.2016, pag. 1.

(101) Dal momento che obblighi ulteriori sono già stati specificati tramite atti delegati e di esecuzione basati su norme tecniche di regolamentazione e di attuazione contenute nei regolamenti (CE) n. 1060/2009 ([23]), (UE) n. 648/2012 ([24]), (UE) n. 600/2014 ([25]) e (UE) n. 909/2014 ([26]) del Parlamento europeo e del Consiglio, è opportuno conferire alle AEV, a livello individuale o collettivo tramite il comitato congiunto, il mandato di sottoporre alla Commissione norme tecniche di regolamentazione e di attuazione in vista dell'adozione di atti delegati e di esecuzione che riprendano e aggiornino le norme vigenti in materia di gestione dei rischi informatici.

(102) Dal momento che il presente regolamento, assieme alla direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio ([27]), comporta il consolidamento delle disposizioni per la gestione dei rischi informatici in una molteplicità di regolamenti e direttive dell'acquis sui servizi finanziari dell'Unione, tra cui i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 e il regolamento (UE) 2016/1011 ([28]) del Parlamento europeo e del Consiglio, per garantire completa coerenza è opportuno modificare tali regolamenti per precisare che le disposizioni applicabili in materia di rischi informatici sono stabilite nel presente regolamento.

(103) È pertanto opportuno limitare l'ambito di applicazione dei pertinenti articoli relativi al rischio operativo, in base ai quali nei regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 era stato conferito il mandato di adottare atti delegati e di esecuzione, allo scopo di riprendere nel presente regolamento tutte le disposizioni sugli aspetti relativi alla resilienza operativa digitale che oggi fanno parte di quei regolamenti.

(104) Il potenziale rischio informatico sistemico connesso all'utilizzo delle infrastrutture di TIC che consentono il funzionamento dei sistemi di pagamento e la prestazione di attività di trattamento dei pagamenti dovrebbe essere debitamente affrontato a livello dell'Unione attraverso norme armonizzate in materia di resilienza digitale. A tal fine, la Commissione dovrebbe valutare rapidamente la necessità di rivedere l'ambito di applicazione del presente regolamento allineando nel contempo tale revisione all'esito del riesame complessivo previsto dalla direttiva (UE) 2015/2366. Numerosi attacchi su vasta scala verificatisi nel corso dell'ultimo decennio dimostrano che i sistemi di pagamento sono diventati esposti alle minacce informatiche. Collocati al centro della catena dei servizi di pagamento e caratterizzati da forti interconnessioni con l'intero sistema finanziario, i sistemi di pagamento e le attività di trattamento dei pagamenti hanno acquisito un'importanza cruciale per il funzionamento dei mercati finanziari dell'Unione. Gli attacchi informatici contro tali sistemi possono causare gravi perturbazioni delle attività a livello operativo, con ripercussioni dirette su funzioni economiche fondamentali, quali l'agevolazione dei pagamenti, e effetti indiretti sui relativi processi economici. Fino all'istituzione a livello dell'Unione di un regime armonizzato e della supervisione degli operatori dei sistemi di pagamento e dei soggetti incaricati del trattamento delle operazioni, gli Stati membri possono, al fine di applicare pratiche di mercato analoghe, trarre ispirazione dai requisiti in materia di resilienza operativa digitale stabiliti dal presente regolamento nell'applicare le norme nei confronti degli operatori di sistemi di pagamento e dei soggetti incaricati del trattamento delle operazioni sottoposti a vigilanza nelle rispettive giurisdizioni.

([23]) 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).

([24]) 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).

([25]) Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84).

([26]) 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).

([27]) Direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (cfr. pag. 153 della presente Gazzetta ufficiale).

([28]) 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).

(105) Poiché l'obiettivo del presente regolamento, ossia il conseguimento di un elevato livello di resilienza operativa digitale per le entità finanziarie regolamentate, non può essere conseguito in misura sufficiente dagli Stati membri, in quanto richiede l'armonizzazione di varie norme differenti nel diritto dell'Unione e nel diritto nazionale, ma, a motivo della portata o degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(106) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([29]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 10 maggio 2021 ([30]),

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

1. Al fine di conseguire un livello comune elevato di resilienza operativa digitale, il presente regolamento stabilisce i seguenti obblighi uniformi in relazione alla sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie:

a) obblighi applicabili alle entità finanziarie in materia di:

   i) gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);

   ii) segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;

   iii) segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;

   iv) test di resilienza operativa digitale;

   v) condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;

   vi) misure relative alla solida gestione dei rischi informatici derivanti da terzi;

b) obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie;

c) norme per l'istituzione e l'attuazione di un quadro di sorveglianza per i fornitori terzi critici di servizi TIC, allorché forniscono i loro servizi a entità finanziarie;

d) norme sulla cooperazione tra autorità competenti e norme sulla vigilanza e l'applicazione da parte delle autorità competenti in relazione a tutte le materie trattate dal presente regolamento.

2. Quanto alle entità finanziarie identificate come soggetti essenziali o importanti ai sensi delle norme nazionali che recepiscono l'articolo 3 della direttiva 2022/2555, il presente regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 4 di tale direttiva.

3. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri per quanto riguarda le funzioni essenziali dello Stato concernenti la sicurezza pubblica, la difesa e la sicurezza nazionale conformemente al diritto dell'Unione.

([29]) 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).

([30]) GU C 229 del 15.6.2021, pag. 16.

Articolo 2

Ambito di applicazione

1. Fatti salvi i paragrafi 3 e 4, il presente regolamento si applica alle entità seguenti:

a) enti creditizi;

b) istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366;

c) prestatori di servizi di informazione sui conti;

d) istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE;

e) imprese di investimento;

f) fornitori di servizi per le cripto-attività autorizzati a norma del regolamento del Parlamento europeo e del Consiglio concernente i mercati delle cripto-attività e recante modifica dei regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e delle direttive 2013/36/UE e (UE) 2019/1937 (regolamento sui mercati delle cripto-attività) ed emittenti di token collegati ad attività;

g) depositari centrali di titoli;

h) controparti centrali;

i) sedi di negoziazione;

j) repertori di dati sulle negoziazioni;

k) gestori di fondi di investimento alternativi;

l) società di gestione;

m) fornitori di servizi di comunicazione dati;

n) imprese di assicurazione e di riassicurazione;

o) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;

p) enti pensionistici aziendali o professionali;

q) agenzie di rating del credito;

r) amministratori di indici di riferimento critici;

s) fornitori di servizi di crowdfunding;

t) repertori di dati sulle cartolarizzazioni;

u) fornitori terzi di servizi TIC.

2. Ai fini del presente regolamento le entità di cui al paragrafo 1 lettere da a) a t) sono definite collettivamente «entità finanziarie».

3. Il presente regolamento non si applica a:

a) gestori di fondi di investimento alternativi di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE;

b) imprese di assicurazione e di riassicurazione di cui all'articolo 4 della direttiva 2009/138/UE;

c) enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che contano congiuntamente non più di 15 aderenti in totale;

d) persone fisiche o giuridiche esentate a norma degli articoli 2 e 3 della direttiva 2014/65/UE;

e) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio che sono microimprese o piccole o medie imprese;

f) uffici dei conti correnti postali di cui all'articolo 2, paragrafo 5, punto 3), della direttiva 2013/36/UE.

4. Gli Stati membri possono escludere dall'ambito di applicazione del presente regolamento le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE che sono situati nei rispettivi territori. Qualora uno Stato membro si avvalga di tale facoltà, e in occasione di ogni successiva modifica, ne informa la Commissione. La Commissione mette tali informazioni a disposizione del pubblico sul suo sito web o attraverso altri canali facilmente accessibili.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni;

2) «sistema informatico e di rete»: un sistema informatico e di rete quali definiti all'articolo 6, punto 1), della direttiva (UE) 2022/2555;

3) «sistema legacy»: un sistema di TIC che ha raggiunto la fine del suo ciclo di vita (fine vita), non si presta ad aggiornamenti o correzioni per motivi tecnologici o commerciali, o non è più supportato dal suo fornitore o da un fornitore terzo di servizi TIC, ma è ancora in uso e supporta le funzioni dell'entità finanziaria;

4) «sicurezza dei sistemi informatici e di rete»: la sicurezza dei sistemi informatici e di rete quale definita all'articolo 6, punto 2), della direttiva (UE) 2022/2555;

5) «rischi informatici»: qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale o fisico;

6) «patrimonio informativo»: una raccolta di informazioni, tangibili o intangibili, che è importante proteggere;

7) «risorse TIC»: software o hardware presenti nei sistemi informatici e di rete utilizzati dall'entità finanziaria;

8) «incidente connesso alle TIC»: un singolo evento, o una serie di eventi collegati non programmati dall'entità finanziaria, che compromette la sicurezza dei sistemi informatici e di rete e ha un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza dei dati o sui servizi forniti dall'entità finanziaria;

9) «incidente operativo o di sicurezza dei pagamenti»: un singolo evento o una serie di eventi collegati non programmati dalle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), connessi alle TIC o meno, che hanno un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza, la disponibilità, l'integrità o l'autenticità dei dati connessi ai pagamenti o sui servizi connessi ai pagamenti forniti dall'entità finanziaria;

10) «grave incidente TIC»: un incidente connesso alle TIC che ha un impatto avverso sui sistemi informatici e di rete a supporto delle funzioni essenziali o importanti dell'entità finanziaria;

11) «grave incidente operativo o di sicurezza dei pagamenti»: un incidente operativo o di sicurezza dei pagamenti che ha un impatto avverso sui servizi connessi ai pagamenti forniti;

12) «minaccia informatica»: minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

13) «minaccia informatica significativa»: una minaccia informatica le cui caratteristiche tecniche indicano che potrebbe potenzialmente causare un grave incidente TIC o un grave incidente operativo o di sicurezza dei pagamenti;

14) «attacco informatico»: un incidente doloso connesso alle TIC provocato dal tentativo, da parte dell'autore della minaccia, di distruggere, rivelare, alterare, disabilitare, rubare o utilizzare senza autorizzazione un'attività o ancora accedervi senza autorizzazione;

15) «analisi delle minacce»: informazioni aggregate, trasformate, analizzate, interpretate o arricchite per offrire il contesto necessario al processo decisionale e consentire conoscenze pertinenti e sufficienti per attenuare l'impatto di un incidente connesso alle TIC o di una minaccia informatica, compresi i dettagli tecnici dell'attacco informatico, i responsabili dell'attacco, il loro modus operandi e le loro motivazioni;

16) «vulnerabilità»: debolezza, predisposizione o difetto di una risorsa, un sistema, un processo o un controllo potenzialmente sfruttabile;

17) «test di penetrazione guidato dalla minaccia (TLPT)»: un quadro che imita le tattiche, le tecniche e le procedure di attori reali della minaccia che sono percepiti come minaccia informatica autentica, che consente di eseguire un test dei sistemi di produzione attivi e critici dell'entità finanziaria in maniera controllata, mirata e basata sull'analisi della minaccia (*red team*);

18) «rischi informatici TIC derivanti da terzi»: rischi relativi alle TIC cui un'entità finanziaria può essere esposta in relazione al ricorso, da parte di questa, a servizi TIC offerti da fornitori terzi o da subappaltatori di tali fornitori, anche mediante accordi di esternalizzazione;

19) «fornitore terzo di servizi TIC»: un'impresa che fornisce servizi TIC;

20) «fornitore intragruppo di servizi TIC»: un'impresa che fa parte di un gruppo finanziario e fornisce prevalentemente servizi TIC a entità finanziarie dello stesso gruppo o a entità finanziarie appartenenti allo stesso sistema di tutela istituzionale (*institutional protection scheme*), comprese le loro società madri, imprese figlie e succursali o altre entità di proprietà comune o sotto controllo comune;

21) «servizi TIC»: servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali;

22) «funzione essenziale o importante»: una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari;

23) «fornitore terzo critico di servizi TIC»: un fornitore terzo di servizi TIC designato come critico in conformità dell'articolo 31;

24) «fornitore terzo di servizi TIC stabilito in un paese terzo»: un fornitore terzo di servizi TIC che è una persona giuridica stabilita in un paese terzo che ha stipulato un accordo contrattuale con un'entità finanziaria per la fornitura di servizi TIC;

25) «impresa figlia»: impresa figlia ai sensi dell'articolo 2, punto 10), e dell'articolo 22 della direttiva 2013/34/UE;

26) «gruppo»: un gruppo quale definito all'articolo 2, punto 11), della direttiva 2013/34/UE;

27) «impresa madre»: impresa madre ai sensi dell'articolo 2, punto 9), e dell'articolo 22 della direttiva 2013/34/UE;

28) «subappaltatore di TIC stabilito in un paese terzo»: un subappaltatore di TIC che è una persona giuridica stabilita in un paese terzo che ha stipulato un accordo contrattuale con un fornitore terzo di servizi TIC o con un fornitore terzo di servizi TIC stabilito in un paese terzo;

29) «rischio di concentrazione delle TIC»: l'esposizione a fornitori terzi critici di servizi TIC, singoli o molteplici e correlati tra loro, che crea un grado di dipendenza tale da detti fornitori che l'indisponibilità, i guasti o altri tipi di carenze che si verificassero presso di essi potrebbero mettere a repentaglio la capacità di un'entità finanziaria di assolvere funzioni essenziali o importanti oppure di assorbire altri tipi di effetti avversi, comprese perdite cospicue, o potrebbero mettere a repentaglio la stabilità finanziaria dell'intera Unione;

30) «organo di gestione»: organo di gestione quale definito all'articolo 4, paragrafo 1, punto 36), della direttiva 2014/65/UE, all'articolo 3, paragrafo 1, punto 7), della direttiva 2013/36/UE, all'articolo 2, paragrafo 1, lettera s), della direttiva 2009/65/CE del Parlamento europeo e del Consiglio ([31]), all'articolo 2, paragrafo 1, punto 45), del regolamento (UE) n. 909/2014, all'articolo 3, paragrafo 1, punto 20), del regolamento (UE) 2016/1011 e alla pertinente disposizione del regolamento sui mercati delle cripto-attività oppure le persone equivalenti che gestiscono di fatto l'entità o che assolvono funzioni chiave conformemente al pertinente diritto dell'Unione o nazionale;

31) «ente creditizio»: ente creditizio ai sensi dell'articolo 4, paragrafo 1, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([32]);

32) «ente esentato dalla direttiva 2013/36/UE»: un'entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE;

33) «impresa di investimento»: un'impresa di investimento quale definita all'articolo 4, paragrafo 1, punto 1), della direttiva 2014/65/UE;

34) «impresa di investimento piccola e non interconnessa»: un'impresa di investimento che soddisfa le condizioni di cui all'articolo 12, paragrafo 1, del regolamento (UE) 2019/2033 del Parlamento europeo e del Consiglio ([33]);

35) «istituto di pagamento»: un istituto di pagamento quale definito all'articolo 4, punto 4), della direttiva (UE) 2015/2366;

36) «istituto di pagamento esentato a norma della direttiva (UE) 2015/2366»: un istituto di pagamento esentato a norma dell'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366;

37) «prestatore di servizi di informazione sui conti»: un prestatore di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366;

38) «istituto di moneta elettronica»: un istituto di moneta elettronica quale definito all'articolo 2, punto 1), della direttiva 2009/110/CE del Parlamento europeo e del Consiglio;

39) «istituto di moneta elettronica esentato a norma della direttiva 2009/110/CE»: un istituto di moneta elettronica; che beneficia di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE;

40) «controparte centrale»: una controparte centrale quale definita all'articolo 2, punto 1), del regolamento (UE) n. 648/2012;

41) «repertorio di dati sulle negoziazioni»: un repertorio di dati sulle negoziazioni quale definito all'articolo 2, punto 2), del regolamento (UE) n. 648/2012;

42) «depositario centrale di titoli»: un depositario centrale di titoli quale definito all'articolo 2, paragrafo 1, punto 1), del regolamento (UE) n. 909/2014;

43) «sede di negoziazione»: una sede di negoziazione quale definita all'articolo 4, paragrafo 1, punto 24), della direttiva 2014/65/UE;

44) «gestore di fondi di investimento alternativi»: un gestore di fondi di investimento alternativi quale definito all'articolo 4, paragrafo 1, lettera b), della direttiva 2011/61/UE;

45) «società di gestione»: una società di gestione quale definita all'articolo 2, paragrafo 1, lettera b), della direttiva 2009/65/CE;

46) «fornitore di servizi di comunicazione dati»: un fornitore di servizi di comunicazione dati ai sensi del regolamento (UE) n. 600/2014, articolo 2, paragrafo 1, punti da 34) a 36);

47) «impresa di assicurazione»: impresa di assicurazione ai sensi dell'articolo 13, punto 1), della direttiva 2009/138/CE;

48) «impresa di riassicurazione»: impresa di riassicurazione ai sensi dell'articolo 13, punto 4), della direttiva 2009/138/CE;

([31]) 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).

([32]) Regolamento (UE) n. 575/2013, del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).

([33]) Regolamento (UE) 2019/2033 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti prudenziali delle imprese di investimento e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 575/2013, (UE) n. 600/2014 e (UE) n. 806/2014 (GU L 314 del 5.12.2019, pag. 1).

49) «intermediario assicurativo»: un intermediario assicurativo quale definito all'articolo 2, paragrafo 1, punto 3), della direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio ([34]);

50) «intermediario assicurativo a titolo accessorio»: un intermediario assicurativo quale definito all'articolo 2, paragrafo 1, punto 4), della direttiva (UE) 2016/97;

51) «intermediario riassicurativo»: un intermediario riassicurativo quale definito all'articolo 2, paragrafo 1, punto 5), della direttiva (UE) 2016/97;

52) «ente pensionistico aziendale o professionale»: un ente pensionistico aziendale o professionale quale definito all'articolo 6, punto 1), della direttiva 2016/2341;

53) «piccolo ente pensionistico aziendale o professionale»: un ente pensionistico aziendale o professionale che gestisce schemi pensionistici che contano congiuntamente meno di 100 aderenti in totale;

54) «agenzia di rating del credito»: un'agenzia di rating del credito quale definita all'articolo 3, paragrafo 1, lettera a), del regolamento (CE) n. 1060/2009;

55) «fornitore di servizi per le cripto-attività»: un fornitore di servizi per le cripto-attività quale definito alla pertinente disposizione del regolamento sui mercati delle cripto-attività;

56) «emittente di token collegati ad attività»: un emittente di token collegati ad attività quale definito alla pertinente disposizione del regolamento sui mercati delle cripto-attività;

57) «amministratore di indici di riferimento critici»: un amministratore di indici di riferimento critici quale definito all'articolo 3, punto 25), del regolamento (UE) 2016/1011;

58) «fornitore di servizi di crowdfunding»: un fornitore di servizi di crowdfunding quale definito all'articolo 2, paragrafo 1, lettera e), del regolamento (UE) 2020/1503 del Parlamento europeo e del Consiglio ([35]);

59) «repertorio di dati sulle cartolarizzazioni»: un repertorio di dati sulle cartolarizzazioni quale definito all'articolo 2, punto 23), del regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio ([36]);

60) «microimpresa»: un'entità finanziaria, diversa da una sede di negoziazione, una controparte centrale, un repertorio di dati sulle negoziazioni o un depositario centrale di titoli, che occupa meno di 10 persone e realizza un fatturato annuo e/o un totale di bilancio annuo non superiore a 2 milioni di EUR;

61) «autorità di sorveglianza capofila»: l'autorità europea di vigilanza designata a norma dell'articolo 31, paragrafo 1, lettera b), del presente regolamento;

62) «comitato congiunto»: il comitato di cui all'articolo 54 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010;

63) «piccola impresa»: un'entità finanziaria che occupa 10 o più persone ma meno di 50 persone e realizza un fatturato annuo e/o un totale di bilancio annuo che supera 2 milioni di EUR ma non superiore a 10 milioni di EUR;

64) «media impresa»: un'entità finanziaria che non è una piccola impresa, occupa meno di 250 persone e realizza un fatturato annuo non superiore a 50 milioni di EUR e/o un bilancio annuo non superiore a 43 milioni di EUR;

65) «autorità pubblica»: qualsiasi ente governativo o altro ente della pubblica amministrazione, comprese le banche centrali nazionali.

([34]) 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).

([35]) 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).

([36]) Regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, che stabilisce un quadro generale per la cartolarizzazione, instaura un quadro specifico per cartolarizzazioni semplici, trasparenti e standardizzate e modifica le direttive 2009/65/CE, 2009/138/CE e 2011/61/UE e i regolamenti (CE) n. 1060/2009 e (UE) n. 648/2012 (GU L 347 del 28.12.2017, pag. 35).

Articolo 4

Principio di proporzionalità

1. Le entità finanziarie attuano le norme di cui al capo II conformemente al principio di proporzionalità, tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività.

2. Inoltre, l'applicazione dei capi III e IV e del capo V, sezione I, da parte delle entità finanziarie è proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, delle loro attività e della loro operatività, come specificamente previsto dalle pertinenti norme di tali capi.

3. Le autorità competenti prendono in considerazione l'applicazione del principio di proporzionalità da parte delle entità finanziarie in sede di riesame della coerenza del quadro per la gestione dei rischi informatici sulla base delle relazioni presentate su richiesta delle autorità competenti a norma dell'articolo 6, paragrafo 5, e dell'articolo 16, paragrafo 2.

CAPO II

Gestione dei rischi informatici

Sezione I

Articolo 5

Governance e organizzazione

1. Le entità finanziarie predispongono un quadro di gestione e di controllo interno che garantisce una gestione efficace e prudente di tutti i rischi informatici, conformemente all'articolo 6, paragrafo 4, al fine di acquisire un elevato livello di resilienza operativa digitale.

2. L'organo di gestione dell'entità finanziaria definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, vigila su tale attuazione e ne è responsabile.

Ai fini del primo comma, l'organo di gestione:

a) assume la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria;

b) predispone politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati;

c) definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC e stabilisce adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni;

d) ha la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale di cui all'articolo 6, paragrafo 8, compresa la determinazione del livello appropriato di tolleranza per i rischi informatici dell'entità finanziaria, ai sensi dell'articolo 6, paragrafo 8, lettera b);

e) approva, supervisiona e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC dell'entità finanziaria, di cui rispettivamente all'articolo 11, paragrafi 1 e 3, che possono essere adottati come politica specifica dedicata che costituisce parte integrante della politica generale di continuità operativa e del piano di risposta e ripristino dell'entità finanziaria;

f) approva e riesamina periodicamente i piani interni di audit in materia di TIC dell'entità finanziaria, gli audit in materia di TIC e le più importanti modifiche a essi apportate;

g) assegna e riesamina periodicamente le risorse finanziarie adeguate per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresi i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale di cui all'articolo 13, paragrafo 6, nonché le competenze in materia di TIC per tutto il personale;

h) approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle modalità per l'uso dei servizi TIC prestati dal fornitore terzo di servizi TIC;

i) istituisce a livello aziendale canali di comunicazione che gli consentono di essere debitamente informato in merito a quanto segue:

   i) gli accordi conclusi con i fornitori terzi di servizi TIC sull'uso di tali servizi;

   ii) le relative eventuali modifiche importanti e pertinenti previste riguardo ai fornitori terzi di servizi TIC;

   iii) il potenziale impatto di tali modiche sulle funzioni essenziali o importanti soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno gli gravi incidenti TIC e il loro impatto, le misure di risposta e ripristino e le misure correttive.

3. Le entità finanziarie diverse dalle microimprese istituiscono un ruolo al fine di monitorare gli accordi conclusi con i fornitori terzi di servizi TIC per l'uso di tali servizi, oppure designano un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente.

4. I membri dell'organo di gestione dell'entità finanziaria mantengono attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, anche seguendo una formazione specifica su base regolare, commisurata ai rischi informatici gestiti.

Sezione II

Articolo 6

Quadro per la gestione dei rischi informatici

1. Nell'ambito del sistema di gestione globale del rischio, le entità finanziarie predispongono un quadro per la gestione dei rischi informatici solido, esaustivo e adeguatamente documentato, che consenta loro di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale.

2. Il quadro per la gestione dei rischi informatici comprende almeno strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere debitamente e adeguatamente tutti i patrimoni informativi e i risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili, così da garantire che tutti i patrimoni informativi e i risorse TIC siano adeguatamente protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati.

3. Conformemente al proprio quadro per la gestione dei rischi informatici, le entità finanziarie riducono al minimo l'impatto dei rischi informatici applicando strategie, politiche, procedure, protocolli e strumenti in materia di TIC adeguati. Forniscono alle autorità competenti, su richiesta di queste ultime, informazioni complete e aggiornate sui rischi informatici e sul proprio quadro per la gestione dei rischi informatici.

4. Le entità finanziarie diverse dalle microimprese attribuiscono la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo, di cui assicurano un livello appropriato d'indipendenza per evitare conflitti d'interessi. Le entità finanziarie garantiscono un'opportuna separazione e indipendenza tra funzioni di gestione dei rischi informatici, funzioni di controllo e funzioni di audit interno, secondo il modello delle tre linee di difesa o secondo un modello interno di controllo e gestione del rischio.

5. Il quadro per la gestione dei rischi informatici è documentato e riesaminato almeno una volta all'anno, o periodicamente in caso di microimprese, nonché in occasione di gravi incidenti TIC e in seguito a indicazioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza operativa digitale o di processi di audit. Il quadro è costantemente migliorato sulla base degli insegnamenti tratti dall'attuazione e dal monitoraggio. È presentata all'autorità competente, su sua richiesta, una relazione in merito al riesame del quadro per la gestione dei rischi informatici.

6. Il quadro per la gestione dei rischi informatici delle entità finanziarie, diverse dalle microimprese, è sottoposto periodicamente a verifiche di audit interne effettuate da addetti all'audit in linea con i piani di audit delle entità finanziarie. Tali addetti all'audit possiedono conoscenze, competenze ed esperienze adeguate in materia di rischi informatici, nonché un'adeguata indipendenza. La frequenza e l'oggetto delle verifiche di audit in materia di TIC sono commisurati ai rischi connessi alle TIC cui è esposta l'entità finanziaria.

7. Sulla base delle conclusioni dell'audit interno in materia di TIC, le entità finanziarie istituiscono un procedimento formale per darvi seguito, comprendente regole per la verifica tempestiva delle risultanze critiche e l'adozione di rimedi.

8. Il quadro per la gestione dei rischi informatici comprende una strategia di resilienza operativa digitale che definisce le modalità di attuazione del quadro. A tal fine, la strategia di resilienza operativa digitale include metodi per affrontare i rischi informatici e conseguire specifici obiettivi in materia di TIC:

a) spiegando in che modo il quadro per la gestione dei rischi informatici sostiene gli obiettivi e la strategia commerciale dell'entità finanziaria;

b) fissando il livello di tolleranza per i rischi informatici, conformemente alla propensione al rischio dell'entità finanziaria e analizzando la tolleranza d'impatto per le perturbazioni a livello di TIC;

c) indicando chiari obiettivi in materia di sicurezza delle informazioni, compresi indicatori chiave di prestazione e parametri chiave di rischio;

d) spiegando l'architettura di riferimento a livello di TIC e le eventuali modifiche necessarie per conseguire specifici obiettivi commerciali;

e) delineando i differenti meccanismi introdotti per individuare incidenti connessi alle TIC, prevenire il loro impatto e proteggersi dallo stesso;

f) documentando l'attuale situazione di resilienza operativa digitale sulla base del numero di gravi incidenti TIC segnalati, nonché l'efficacia delle misure preventive;

g) attuando test di resilienza operativa digitale, conformemente al capo IV del presente regolamento;

h) delineando una strategia di comunicazione in caso di incidenti connessi alle TIC di cui è richiesta la divulgazione a norma dell'articolo 14.

9. Le entità finanziarie possono, nel contesto della strategia di resilienza operativa digitale di cui al paragrafo 8, definire una strategia olistica per le TIC a livello di gruppo o di entità, basata su una varietà di fornitori, che indichi le principali dipendenze da fornitori terzi di servizi TIC e che spieghi la logica sottesa alla ripartizione degli appalti tra i fornitori terzi di servizi TIC.

10. Le entità finanziarie possono, conformemente alla normativa settoriale dell'Unione e nazionale, esternalizzare a imprese interne o esterne al gruppo i compiti di verifica della conformità ai requisiti in materia di gestione dei rischi informatici. In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di verificare la conformità ai requisiti in materia di gestione dei rischi informatici.

Articolo 7

Sistemi, protocolli e strumenti di TIC

Al fine di affrontare e gestire i rischi informatici, le entità finanziarie utilizzano e mantengono aggiornati sistemi, protocolli e strumenti di TIC che sono:

a) idonei alle dimensioni delle operazioni a supporto dello svolgimento delle attività delle entità finanziarie, conformemente al principio di proporzionalità di cui all'articolo 4;

b) affidabili;

c) dotati di capacità sufficiente per elaborare in maniera accurata i dati necessari per lo svolgimento delle attività e la tempestiva fornitura dei servizi, nonché per sostenere i picchi di volume di ordini, messaggi od operazioni, a seconda delle necessità, anche in caso di introduzione di nuove tecnologie;

d) tecnologicamente resilienti, in modo da fare adeguatamente fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse.

Articolo 8

Identificazione

1. Nell'ambito del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie identificano, classificano e documentano adeguatamente tutte le funzioni commerciali supportate dalle TIC, i ruoli e le responsabilità, i patrimoni informativi e le risorse TIC a supporto delle suddette funzioni, nonché i ruoli e le dipendenze rispettivi in materia di rischi informatici. Le entità finanziarie riesaminano, secondo necessità e almeno una volta all'anno, l'adeguatezza di tale classificazione e di altri documenti eventualmente pertinenti.

2. Le entità finanziarie identificano costantemente tutte le fonti di rischio relative alle TIC, in particolare l'esposizione al rischio da e verso altre entità finanziarie, e valutano le minacce informatiche e le vulnerabilità in materia di TIC pertinenti per le loro funzioni commerciali supportate dalle TIC, per i loro patrimoni informativi e per i loro risorse TIC. Le entità finanziarie riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio che esercitano un impatto su di loro.

3. Le entità finanziarie diverse dalle microimprese effettuano una valutazione del rischio in occasione di ogni modifica di rilievo dell'infrastruttura del sistema informatico e di rete, dei processi o delle procedure che incidono sulle loro funzioni commerciali supportate dalle TIC, sui loro patrimoni informativi o sulle loro risorse TIC.

4. Le entità finanziarie identificano tutti i patrimoni informativi e le risorse TIC, compresi quelli su siti remoti, le risorse di rete e le attrezzature hardware, e mappano quelle considerate essenziali. Effettuano la mappatura della configurazione dei patrimoni informativi e delle risorse TIC, nonché dei collegamenti e delle interdipendenze tra i diversi patrimoni informativi e risorse TIC.

5. Le entità finanziarie identificano e documentano tutti i processi dipendenti da fornitori terzi di servizi TIC e identificano le interconnessioni con detti fornitori che offrono servizi a supporto di funzioni essenziali o importanti.

6. Ai fini dei paragrafi 1, 4 e 5, le entità finanziarie mantengono inventari pertinenti e li aggiornano periodicamente e in occasione di ogni modifica di rilievo di cui al paragrafo 3.

7. Le entità finanziarie diverse dalle microimprese effettuano periodicamente, almeno una volta all'anno e in ogni caso prima e dopo la connessione di tecnologie, applicazioni o sistemi, una valutazione del rischio specifica per tutti i sistemi legacy.

Articolo 9

Protezione e prevenzione

1. Allo scopo di proteggere adeguatamente i sistemi di TIC e nella prospettiva di organizzare misure di risposta, le entità finanziarie monitorano e controllano costantemente la sicurezza e il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto dei rischi informatici sui sistemi di TIC adottando politiche, procedure e strumenti adeguati per la sicurezza delle TIC.

2. Le entità finanziarie definiscono, acquisiscono e attuano politiche, procedure, protocolli e strumenti per la sicurezza delle TIC miranti a garantire la resilienza, la continuità e la disponibilità dei sistemi di TIC, in particolare quelli a supporto di funzioni essenziali o importanti, nonché a mantenere standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati conservati, in uso o in transito.

3. Al fine di conseguire gli obiettivi di cui al paragrafo 2 le entità finanziarie usano soluzioni e processi TIC appropriati conformemente all'articolo 4. Tali soluzioni e processi TIC:

a) garantiscono la sicurezza dei mezzi di trasferimento dei dati;

b) riducono al minimo i rischi di corruzione o perdita di dati, di accesso non autorizzato nonché di difetti tecnici che possono ostacolare l'attività commerciale;

c) prevengono la mancanza di disponibilità, il deterioramento dell'autenticità o dell'integrità, le violazioni della riservatezza e la perdita di dati;

d) assicurano la protezione dei dati contro i rischi derivanti dalla gestione dei dati, compresi la cattiva amministrazione, i rischi relativi al trattamento dei dati e l'errore umano.

4. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie:

a) elaborano e documentano una politica di sicurezza dell'informazione che definisce le norme per tutelare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, dei patrimoni informativi e delle risorse TIC, compresi quelli dei loro clienti, se del caso;

b) seguendo un approccio basato sul rischio, realizzano una solida struttura di gestione della rete e delle infrastrutture impiegando tecniche, metodi e protocolli adeguati, che possono includere l'applicazione di meccanismi automatizzati, per isolare i patrimoni informativi colpiti in caso di attacchi informatici;

c) attuano politiche che limitano l'accesso fisico o logico ai patrimoni informativi e alle risorse TIC unicamente a quanto è necessario per funzioni e attività legittime e approvate, e stabiliscono a tale scopo una serie di politiche, procedure e controlli concernenti i diritti di accesso e garantiscono una solida amministrazione degli stessi;

d) attuano politiche e protocolli riguardanti robusti meccanismi di autenticazione, basati su norme pertinenti e sistemi di controllo dedicati, e misure di protezione delle chiavi crittografiche di cifratura dei dati sulla scorta dei risultati di processi approvati per la classificazione dei dati e la valutazione dei rischi informatici;

e) attuano politiche, procedure e controlli documentati per la gestione delle modifiche delle TIC, comprese le modifiche apportate a componenti software, hardware e firmware, sistemi o parametri di sicurezza, che adottano un approccio basato sulla valutazione del rischio e sono parte integrante del processo complessivo di gestione delle modifiche dell'entità finanziaria, in modo che tutte le modifiche apportate ai sistemi di TIC siano registrate, testate, valutate, approvate, attuate e verificate in maniera controllata;

f) si dotano di politiche documentate, idonee ed esaustive in materia di correzioni ed aggiornamenti.

Ai fini della lettera b) del primo comma, le entità finanziarie progettano l'infrastruttura di connessione di rete in modo che sia possibile isolarla o segmentarla istantaneamente, al fine di ridurre al minimo e prevenire il contagio, soprattutto per i processi finanziari interconnessi.

Ai fini della lettera e) del primo comma, il processo di gestione delle modifiche delle TIC è approvato da linee di gestione adeguate e comprende protocolli specifici in essere.

Articolo 10

Individuazione

1. Le entità finanziarie predispongono meccanismi per individuare tempestivamente le attività anomale, conformemente all'articolo 17, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché per individuare i potenziali singoli punti di vulnerabilità (*points of failure*) importanti.

Tutti i meccanismi di individuazione di cui al primo comma sono periodicamente testati in conformità dell'articolo 25.

2. I meccanismi di individuazione di cui al paragrafo 1 prevedono molteplici livelli di controllo, definiscono soglie di allarme e criteri per l'attivazione e l'avvio dei processi di risposta agli incidenti connessi alle TIC, compresi meccanismi di allarme automatico per il personale incaricato della risposta agli incidenti connessi alle TIC.

3. Le entità finanziarie dedicano risorse e capacità sufficienti al monitoraggio dell'attività degli utenti e di eventuali anomalie e incidenti connessi alle TIC, in particolare attacchi informatici.

4. I fornitori di servizi di comunicazione dati predispongono inoltre sistemi in grado di controllare efficacemente le comunicazioni sulle operazioni per verificarne la completezza, individuare omissioni ed errori palesi e chiederne la ritrasmissione.

Articolo 11

Risposta e ripristino

1. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, e in base ai requisiti di identificazione stabiliti all'articolo 8, le entità finanziarie predispongono una politica di continuità operativa delle TIC esaustiva, la quale può essere adottata come una politica specifica dedicata che costituisce parte integrante della politica generale di continuità operativa dell'entità finanziaria.

2. Le entità finanziarie attuano la politica di continuità operativa delle TIC tramite accordi, piani, procedure e meccanismi appositi, appropriati e documentati, miranti a:

a) garantire la continuità delle funzioni essenziali o importanti dell'entità finanziaria;

b) rispondere in maniera rapida, appropriata ed efficace e trovare una soluzione a tutti gli incidenti connessi alle TIC, in modo da limitare i danni e privilegiare la ripresa delle attività e le azioni di ripristino;

c) attivare senza ritardo piani dedicati che prevedano tecnologie, processi e misure di contenimento idonei a ciascun tipo di incidente connesso alle TIC e a scongiurare danni ulteriori, nonché procedure mirate di risposta e ripristino stabilite in conformità dell'articolo 12;

d) stimare in via preliminare impatti, danni e perdite;

e) stabilire azioni di comunicazione e gestione delle crisi che assicurino la trasmissione di informazioni aggiornate a tutto il personale interno interessato e ai portatori di interessi esterni, conformemente all'articolo 14, e comunicare tali informazioni alle autorità competenti, conformemente all'articolo 19.

3. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie attuano i piani di risposta e ripristino relativi alle TIC associati; per le entità finanziarie diverse dalle microimprese tali piani sono soggetti a un audit interno indipendente.

4. Le entità finanziarie predispongono, mantengono e testano periodicamente opportuni piani di continuità operativa delle TIC, in particolare per quanto riguarda le funzioni essenziali o importanti esternalizzate o appaltate tramite accordi con fornitori terzi di servizi TIC.

5. Nell'ambito della politica generale di continuità operativa, le entità finanziarie effettuano un'analisi dell'impatto sulle attività aziendali (*Business Impact Analysis* — BIA) delle loro esposizioni a gravi perturbazioni delle attività. Nel quadro della BIA, le entità finanziarie valutano l'impatto potenziale di gravi perturbazioni delle attività mediante criteri quantitativi e qualitativi, utilizzando, se del caso, dati interni ed esterni e analisi di scenario. La BIA tiene conto della criticità delle funzioni commerciali, dei processi di supporto, delle dipendenze da terzi e dei patrimoni informativi individuati e mappati, nonché delle loro interdipendenze. Le entità finanziarie provvedono affinché le risorse TIC e i servizi TIC siano progettati e utilizzati in piena conformità con la BIA, in particolare garantendo adeguatamente la ridondanza di tutte le componenti essenziali.

6. All'interno della gestione complessiva dei rischi informatici, le entità finanziarie:

a) testano i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC in relazione ai sistemi di TIC a supporto di tutte le funzioni almeno una volta all'anno nonché in caso di modifiche di rilievo ai sistemi di TIC a supporto di funzioni essenziali o importanti;

b) testano i piani di comunicazione delle crisi istituiti in conformità dell'articolo 14.

Ai fini del primo comma, lettera a), le entità finanziarie diverse dalle microimprese inseriscono nei piani dei test scenari di attacchi informatici e del passaggio tra le infrastrutture delle TIC primarie e la capacità ridondante, i backup e le attrezzature ridondanti necessarie per soddisfare gli obblighi di cui all'articolo 12.

Le entità finanziarie riesaminano periodicamente la politica di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC, tenendo conto dei risultati dei test svolti in conformità del primo comma e delle raccomandazioni formulate sulla base dei controlli di audit o degli esami di vigilanza.

7. Le entità finanziarie diverse dalle microimprese si dotano di una funzione di gestione delle crisi che, in caso di attivazione dei piani di continuità operativa delle TIC o dei piani di risposta e ripristino relativi alle TIC, fissa, tra l'altro, procedure chiare per la gestione della comunicazione interna ed esterna delle crisi, in conformità dell'articolo 14.

8. Le entità finanziarie rendono prontamente accessibili le registrazioni delle attività svolte prima e durante le perturbazioni in cui vengono attivati i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC.

9. Le controparti centrali trasmettono alle autorità competenti copie dei risultati dei test di continuità operativa delle TIC o di esercizi analoghi.

10. Le entità finanziarie, diverse dalle microimprese, comunicano alle autorità competenti, su loro richiesta di queste ultime, una stima dei costi e delle perdite annuali aggregati causati da incidenti gravi connessi alle TIC.

11. A norma dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV elaborano, tramite il comitato congiunto, entro il 17 luglio 2024 orientamenti comuni sulla stima dei costi e delle perdite annuali aggregati di cui al paragrafo 10.

Articolo 12

Politiche e procedure di backup — Procedure e metodi di ripristino e recupero

1. Al fine di assicurare che i sistemi e i dati di TIC siano ripristinati riducendo al minimo il periodo di inattività e limitando la perturbazione e le perdite, all'interno del proprio quadro per la gestione dei rischi informatici le entità finanziarie elaborano e documentano:

a) le politiche e procedure di backup che precisano il perimetro dei dati soggetti a backup e la frequenza minima del backup, in base alla criticità delle informazioni o al livello di riservatezza dei dati;

b) le procedure e i metodi di ripristino e recupero.

2. Le entità finanziarie si dotano di sistemi di backup che possono essere attivati conformemente alle politiche e alle procedure di backup, come pure alle procedure e ai metodi di ripristino e recupero. L'attivazione dei sistemi di backup non mette a repentaglio la sicurezza dei sistemi informatici e di rete né, la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati. I test delle procedure di backup e di ripristino nonché delle procedure e dei metodi di recupero sono effettuati periodicamente.

3. Nel ripristino dei dati di backup effettuato utilizzando i propri sistemi, le entità finanziarie impiegano sistemi di TIC che sono fisicamente e logicamente segregati dal sistema di TIC sorgente. I sistemi di TIC sono protetti in maniera sicura da qualsiasi accesso non autorizzato o corruzione delle TIC e consentono il tempestivo ripristino dei servizi attraverso il backup dei dati e dei sistemi ove necessario.

Per le controparti centrali, i piani di ripristino consentono il ripristino di tutte le operazioni in corso al momento della perturbazione, così da permettere alla controparte centrale di continuare a operare con certezza e di completare la liquidazione alla data programmata.

I fornitori di servizi di comunicazione dati mantengono inoltre risorse adeguate e dispongono di attrezzature di back-up e ripristino per offrire e mantenere in ogni momento i loro servizi.

4. Le entità finanziarie, diverse dalle microimprese, mantengono capacità di TIC ridondanti, dotate di risorse e funzioni sufficienti e adeguate a soddisfare le esigenze commerciali. Le microimprese valutano la necessità di mantenere tali capacità di TIC ridondanti sulla base del loro profilo di rischio.

5. I depositari centrali di titoli mantengono almeno un sito secondario di trattamento dati dotato di risorse, capacità, funzioni e personale adeguati a soddisfare le esigenze commerciali.

Il sito secondario di trattamento dati è:

a) ubicato geograficamente a distanza dal sito primario per garantire che esso abbia un profilo di rischio distinto e impedire che venga colpito dall'evento che ha interessato il sito primario;

b) in grado di garantire la continuità delle funzioni essenziali o importanti in maniera identica al sito primario, oppure di fornire il livello di servizi necessario a garantire che l'entità finanziaria svolga le proprie operazioni essenziali nell'ambito degli obiettivi di ripristino;

c) immediatamente accessibile al personale dell'entità finanziaria per garantire la continuità delle funzioni essenziali o importanti qualora il sito primario di trattamento dati divenga indisponibile.

6. Nel determinare gli obiettivi in materia di punti di ripristino e tempi di ripristino di ciascuna funzione, le entità finanziarie tengono conto del fatto che si tratti di una funzione essenziale o importante e del potenziale impatto complessivo sull'efficienza del mercato. Questi obiettivi in materia di tempi garantiscono che i livelli di servizi concordati siano rispettati anche in scenari estremi.

7. Durante il ripristino successivo a un incidente connesso alle TIC, le entità finanziarie effettuano le verifiche necessarie, comprese eventuali verifiche multiple e controlli incrociati, per assicurare che sia mantenuto il più elevato livello di integrità dei dati. Questi controlli sono effettuati anche al momento di ricostruire i dati provenienti da portatori di interessi esterni, per assicurare la piena coerenza di tutti i dati tra i sistemi.

Articolo 13

Apprendimento ed evoluzione

1. Le entità finanziare dispongono capacità e personale per raccogliere informazioni in relazione alle vulnerabilità e alle minacce informatiche, agli incidenti connessi alle TIC, in particolare agli attacchi informatici, e analizzarne i probabili effetti sulla loro resilienza operativa digitale.

2. Dopo che un grave incidente connesso alle TIC ha perturbato le loro attività principali, le entità finanziarie svolgono un riesame successivo a tale incidente che analizzi le cause della perturbazione e identifichi i miglioramenti che è necessario apportare alle operazioni riguardanti le TIC o nell'ambito della politica di continuità operativa delle TIC di cui all'articolo 11.

Le entità finanziarie diverse dalle microimprese comunicano, su richiesta, alle autorità competenti le modifiche attuate a seguito del riesame successivo all'incidente connesso alle TIC di cui al primo comma.

Il riesame successivo all'incidente connesso alle TIC di cui al primo comma determina se le procedure stabilite siano state seguite e se le azioni adottate siano state efficaci, anche in relazione:

a) alla tempestività della risposta agli allarmi di sicurezza e alla determinazione dell'impatto degli incidenti connessi alle TIC e della loro gravità;

b) alla qualità e alla rapidità dell'analisi forense, ove ritenuto opportuno;

c) all'efficacia della procedura di attivazione dei livelli successivi di intervento in caso di incidenti all'interno dell'entità finanziaria;

d) all'efficacia della comunicazione interna ed esterna.

3. Gli insegnamenti tratti dai test sulla resilienza operativa digitale effettuati in conformità degli articoli 26 e 27 e da incidenti connessi alle TIC realmente avvenuti, in particolare attacchi informatici, insieme alle difficoltà riscontrate al momento dell'attivazione dei piani di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC, nonché le informazioni pertinenti scambiate con le controparti e valutate nel corso degli esami di vigilanza sono debitamente e costantemente integrati nel processo di valutazione dei rischi informatici. Tali risultanze costituiscono la base per opportune revisioni delle relative componenti del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1.

4. Le entità finanziarie monitorano l'efficacia dell'attuazione della loro strategia di resilienza operativa digitale stabilita all'articolo 6, paragrafo 8. Tracciano l'evoluzione nel tempo dei rischi informatici, analizzano la frequenza, i tipi, le dimensioni e l'evoluzione degli incidenti connessi alle TIC, in particolare gli attacchi informatici e i relativi schemi, al fine di comprendere il livello di esposizione ai rischi informatici — segnatamente in relazione alle funzioni essenziali o importanti — e migliorare la maturità informatica e la preparazione dell'entità finanziaria.

5. Il personale addetto alle TIC di grado più elevato comunica almeno una volta all'anno all'organo di gestione le risultanze di cui al paragrafo 3 e formula raccomandazioni.

6. Le entità finanziarie elaborano programmi di sensibilizzazione sulla sicurezza delle TIC nonché attività di formazione sulla resilienza operativa digitale, che rappresentano moduli obbligatori nei programmi di formazione del personale. Tali programmi e attività di formazione riguardano tutti i dipendenti e gli alti dirigenti, e presentano un livello di complessità commisurato all'ambito delle loro funzioni. Se del caso, le entità finanziarie includono anche i fornitori terzi di servizi TIC nei loro sistemi di formazione pertinenti, conformemente all'articolo 30, paragrafo 2, lettera i).

7. Le entità finanziarie diverse dalle microimprese monitorano costantemente i pertinenti sviluppi tecnologici, anche al fine di comprendere i possibili effetti dell'impiego di tali nuove tecnologie sui requisiti in materia di sicurezza delle TIC e sulla resilienza operativa digitale. Si tengono aggiornate sui più recenti processi di gestione dei rischi informatici, in modo da contrastare efficacemente le forme nuove o già esistenti di attacchi informatici.

Articolo 14

Comunicazione

1. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie predispongono piani di comunicazione delle crisi che consentano una divulgazione responsabile di informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità ai clienti e alle controparti nonché al pubblico, a seconda dei casi.

2. All'interno del quadro per la gestione dei rischi informatici, le entità finanziarie attuano politiche di comunicazione per il personale interno e per i portatori di interessi esterni. Le politiche di comunicazione per il personale tengono conto dell'esigenza di operare un distinguo tra il personale coinvolto nella gestione dei rischi informatici, in particolare il personale responsabile della risposta e del ripristino, e il personale che è necessario informare.

3. Nell'entità finanziaria vi è almeno una persona incaricata di attuare la strategia di comunicazione per gli incidenti connessi alle TIC e assolvere a tal fine la funzione di informazione al pubblico e ai media.

Articolo 15

Ulteriore armonizzazione di strumenti, metodi, processi e politiche di gestione del rischio informatico

Tramite il comitato congiunto e in consultazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), le AEV elaborano progetti di norme tecniche di regolamentazione comuni al fine di:

a) specificare ulteriori elementi da inserire nelle strategie, nelle politiche, nelle procedure, nei protocolli e negli strumenti in materia di sicurezza delle TIC di cui all'articolo 9, paragrafo 2, allo scopo di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro le intrusioni e l'uso improprio dei dati, preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, inserire tecniche crittografiche e assicurare un'accurata e pronta trasmissione dei dati senza gravi perturbazioni né indebiti ritardi;

b) sviluppare ulteriori componenti dei controlli sui diritti di gestione dell'accesso di cui all'articolo 9, paragrafo 4, lettera c), e della relativa politica di risorse umane, precisando i diritti di accesso, le procedure per concedere e revocare i diritti, il monitoraggio di comportamenti anomali in relazione ai rischi informatici mediante indicatori appropriati, compresi i modelli di utilizzo della rete, gli orari, l'attività informatica e i dispositivi sconosciuti;

c) elaborare ulteriormente i meccanismi specificati all'articolo 10, paragrafo 1, in modo da consentire un'individuazione tempestiva delle attività anomale, e i criteri di cui all'articolo 10, paragrafo 2, per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi;

d) specificare ulteriormente le componenti della politica di continuità operativa delle TIC di cui all'articolo 11, paragrafo 1;

e) specificare ulteriormente i test sui piani di continuità operativa delle TIC di cui all'articolo 11, paragrafo 6, per garantire che tali test tengano debitamente conto degli scenari in cui la qualità dell'esercizio di una funzione essenziale o importante si deteriora a un livello inaccettabile o viene meno, e che considerino adeguatamente il potenziale impatto dell'insolvenza o di altre disfunzioni di pertinenti fornitori terzi di servizi TIC e, se del caso, i rischi politici nelle giurisdizioni dei rispettivi fornitori;

f) specificare ulteriormente le componenti dei piani di risposta e ripristino relativi alle TIC di cui all'articolo 11, paragrafo 3;

g) specificare ulteriormente il contenuto e il formato della relazione sul riesame del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 5.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, tenendo debitamente conto di eventuali caratteristiche specifiche derivanti dalla natura distinta delle attività nei diversi settori dei servizi finanziari.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 16

Quadro semplificato per la gestione dei rischi informatici

1. Gli articoli da 5 a 15 del presente regolamento non si applicano alle imprese di investimento piccole e non interconnesse e agli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366; agli istituti esentati a norma della direttiva 2013/36/UE per i quali gli Stati membri hanno deciso di non applicare l'opzione di cui all'articolo 2, paragrafo 4, del presente regolamento; agli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE; e ai piccoli enti pensionistici aziendali o professionali.

Fermo restando il primo comma, le entità elencate al primo comma:

a) pongono in essere e mantengono un solido e documentato quadro per la gestione dei rischi informatici che precisa i meccanismi e le misure finalizzate a una gestione rapida, efficiente e organica dei rischi informatici, anche ai fini della protezione delle pertinenti infrastrutture e componenti fisiche;

b) monitorano costantemente la sicurezza e il funzionamento di tutti i sistemi di TIC;

c) riducono al minimo l'impatto dei rischi informatici attraverso l'uso di sistemi, protocolli e strumenti di TIC solidi, resilienti e aggiornati e atti a supportare lo svolgimento delle loro attività e la fornitura di servizi e a proteggere adeguatamente la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati nei sistemi informatici e di rete;

d) provvedono a che le fonti di rischi informatici e le anomalie dei sistemi informatici e di rete siano tempestivamente individuate e rilevate e che gli incidenti connessi alle TIC siano trattati con rapidità;

e) individuano le principali dipendenze da fornitori terzi di servizi TIC;

f) garantiscono la continuità delle funzioni essenziali o importanti, attraverso piani di continuità operativa e misure di risposta e recupero, che comprendano almeno misure di back-up e ripristino;

g) testano periodicamente i piani e le misure di cui alla lettera f) nonché l'efficacia dei controlli attuati in conformità delle lettere a) e c);

h) attuano, se del caso, le opportune conclusioni operative risultanti dai test di cui alla lettera g) e dall'analisi successiva all'incidente nel processo di valutazione dei rischi informatici ed elaborano, in funzione delle esigenze e del profilo dei rischi informatici, programmi di formazione e sensibilizzazione sulla sicurezza delle TIC per il personale e la dirigenza.

2. Il quadro per la gestione dei rischi informatici di cui al paragrafo 1, secondo comma, lettera a), è documentato e riesaminato periodicamente e al verificarsi di incidenti gravi connessi alle TIC conformemente alle istruzioni delle autorità di vigilanza. Il quadro è costantemente migliorato sulla base degli insegnamenti tratti dall'attuazione e dal monitoraggio. Su sua richiesta, è presentata all'autorità competente una relazione sul riesame del quadro per la gestione dei rischi informatici.

3. Tramite il comitato congiunto e in consultazione con l'ENISA, le AEV elaborano progetti di norme tecniche di regolamentazione comuni al fine di:

a) specificare ulteriormente gli elementi da includere nel quadro per la gestione dei rischi informatici di cui al paragrafo 1, secondo comma, lettera a);

b) specificare ulteriormente gli elementi relativi ai sistemi, ai protocolli e agli strumenti per ridurre al minimo l'impatto dei rischi informatici di cui al paragrafo 1, secondo comma, lettera c), allo scopo di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro le intrusioni e l'uso improprio dei dati e preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati;

c) specificare ulteriormente le componenti dei piani di continuità operativa delle TIC di cui al paragrafo 1, secondo comma, lettera f);

d) specificare ulteriormente le norme riguardanti i test sui piani di continuità operativa e assicurare l'efficacia dei controlli di cui al paragrafo 1, secondo comma, lettera g), e garantire che tali test tengano debitamente conto degli scenari in cui la qualità dell'esercizio di una funzione essenziale o importante si deteriora a un livello inaccettabile o viene meno;

e) specificare ulteriormente il contenuto e il formato della relazione sul riesame del quadro per la gestione dei rischi informatici di cui al paragrafo 2.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

CAPO III

Gestione, classificazione e segnalazione degli incidenti informatici

Articolo 17

Processo di gestione degli incidenti connessi alle TIC

1. Le entità finanziarie definiscono, stabiliscono e attuano un processo di gestione degli incidenti connessi alle TIC al fine di individuare, gestire e notificare tali incidenti.

2. Le entità finanziarie registrano tutti gli incidenti connessi alle TIC e le minacce informatiche significative. Le entità finanziarie istituiscono procedure e processi appropriati per garantire, in maniera coerente e integrata, il monitoraggio e il trattamento degli incidenti connessi alle TIC, nonché il relativo seguito, in modo da identificare, documentare e affrontare le cause di fondo e prevenire il verificarsi di tali incidenti.

3. Il processo di gestione degli incidenti connessi alle TIC di cui al paragrafo 1:

a) predispone indicatori di allerta precoce;

b) stabilisce procedure per identificare, tracciare, registrare, categorizzare e classificare gli incidenti connessi alle TIC in base alla loro priorità e gravità e in base alla criticità dei servizi colpiti, conformemente ai criteri di cui all'articolo 18, paragrafo 1;

c) assegna i ruoli e le responsabilità che è necessario attivare per i diversi scenari e tipi di incidenti connessi alle TIC;

d) elabora piani per la comunicazione al personale, ai portatori di interessi esterni e ai mezzi di comunicazione conformemente all'articolo 14, nonché per la notifica ai clienti, per le procedure di attivazione dei livelli successivi di intervento, compresi i reclami dei clienti in materia di TIC, e per la comunicazione di informazioni alle entità finanziarie che agiscono da controparti, a seconda dei casi;

e) assicura la segnalazione almeno degli incidenti gravi connessi alle TIC agli alti dirigenti interessati e informa l'organo di gestione almeno in merito a detti incidenti, illustrandone l'impatto e la risposta e i controlli supplementari da introdurre;

f) stabilisce procedure di risposta agli incidenti connessi alle TIC per attenuarne l'impatto e garantisce tempestivamente l'operatività e la sicurezza dei servizi.

Articolo 18

Classificazione degli incidenti connessi alle TIC e delle minacce informatiche

1. Le entità finanziarie classificano gli incidenti connessi alle TIC e ne determinano l'impatto in base ai criteri seguenti:

a) il numero e/o la rilevanza di clienti o controparti finanziarie interessati e, ove applicabile, la quantità o il numero di transazioni interessate dall'incidente connesso alle TIC e il fatto che tale incidente abbia provocato o meno un impatto reputazionale;

b) la durata dell'incidente connesso alle TIC, compreso il periodo di inattività del servizio;

c) l'estensione geografica dell'incidente connesso alle TIC, con riferimento alle aree colpite, in particolare se interessa più di due Stati membri;

d) le perdite di dati derivanti dall'incidente connesso alle TIC, in relazione alla disponibilità, autenticità, integrità o riservatezza dei dati;

e) la criticità dei servizi colpiti, comprese le operazioni dell'entità finanziaria;

f) l'impatto economico dell'incidente connesso alle TIC — in particolare le perdite e i costi diretti e indiretti — in termini sia assoluti che relativi.

2. Le entità finanziarie classificano le minacce informatiche come significative in base alla criticità dei servizi a rischio, comprese le operazioni dell'entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio.

3. In consultazione con la BCE e l'ENISA, le AEV elaborano, tramite il comitato congiunto, progetti di norme tecniche di regolamentazione comuni che specificano ulteriormente gli aspetti seguenti:

a) i criteri di cui al paragrafo 1, comprese le soglie di rilevanza per la determinazione dei gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti, che sono oggetto dell'obbligo di segnalazione di cui all'articolo 19, paragrafo 1;

b) i criteri che le autorità competenti devono applicare per valutare la rilevanza degli gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti per le autorità competenti interessate in altri Stati membri, nonché i dettagli delle segnalazioni di incidenti gravi connessi alle 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.

c) i criteri di cui al paragrafo 2 del presente articolo, comprese soglie di rilevanza elevate per la determinazione delle minacce informatiche significative.

4. All'atto dell'elaborazione dei progetti di norme tecniche di regolamentazione comuni di cui al paragrafo 3 del presente articolo, le AEV tengono conto dei criteri di cui all'articolo 4, paragrafo 2, come pure delle norme internazionali, degli orientamenti e delle specifiche elaborati e pubblicati dall'ENISA, tra cui, se del caso, le specifiche riguardanti altri settori economici. Ai fini dell'applicazione dei criteri di cui all'articolo 4, paragrafo 2, le AEV tengono debitamente conto della necessità delle microimprese e delle piccole e medie imprese di mobilitare risorse e capacità sufficienti per garantire una gestione rapida degli incidenti connessi alle TIC.

Le AEV presentano tali progetti di norme tecniche di regolamentazione comuni alla Commissione entro il 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 3 in conformità degli articoli da 0 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 19

Segnalazione dei gravi incidenti TIC e notifica volontaria delle minacce informatiche significative

1. Le entità finanziarie segnalano gli gravi incidenti TIC all'autorità competente interessata di cui all'articolo 46 a norma del paragrafo 4 del presente articolo.

Se un'entità finanziaria è soggetta alla vigilanza di più di un'autorità nazionale competente di cui all'articolo 46, gli Stati membri designano un'unica autorità competente quale autorità competente interessata responsabile dell'espletamento delle funzioni e dei compiti di cui al presente articolo.

Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 segnalano i gravi incidenti TIC all'autorità nazionale competente designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente tale segnalazione alla BCE.

Ai fini del primo comma, le entità finanziarie redigono, dopo aver raccolto e analizzato tutte le informazioni pertinenti, la notifica iniziale e le relazioni di cui al paragrafo 4 del presente articolo utilizzando i modelli di cui all'articolo 20 e le trasmettono all'autorità competente. Qualora un impedimento tecnico non consenta la trasmissione della notifica iniziale utilizzando il modello, le entità finanziarie informano in merito l'autorità competente con mezzi alternativi.

La notifica iniziale e le relazioni di cui al paragrafo 4 contengono tutte le informazioni necessarie all'autorità competente per determinare la rilevanza dell'grave incidente TIC e valutarne i possibili impatti transfrontalieri.

Fatta salva la segnalazione a norma del primo comma da parte dell'entità finanziaria all'autorità competente interessata, gli Stati membri possono stabilire, in aggiunta, che alcune o tutte le entità finanziarie forniscano altresì la notifica iniziale e ciascuna relazione di cui al paragrafo 4 del presente articolo utilizzando i modelli di cui all'articolo 20 alle autorità competenti o ai gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — CSIRT) designati o istituiti a norma della direttiva (UE) 2022/2555.

2. Le entità finanziarie possono, su base volontaria, notificare le minacce informatiche significative all'autorità competente interessata qualora ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti. L'autorità competente interessata può fornire tali informazioni alle altre autorità pertinenti di cui al paragrafo 6.

Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 possono notificare, su base volontaria, le minacce informatiche significative all'autorità nazionale competente, designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente la notifica alla BCE.

Gli Stati membri possono stabilire che le entità finanziarie che procedono alla notifica su base volontaria e a norma del primo comma possano altresì trasmettere tale notifica ai CSIRT nazionali designati o istituiti a norma della direttiva (UE) 2022/2555.

3. Qualora si verifichi un grave incidente TIC che eserciti un impatto sugli interessi finanziari dei clienti, le entità finanziarie, senza indebito ritardo e non appena ne vengono a conoscenza, informano i loro clienti in merito a tale incidente e alle misure che sono state adottate per attenuare gli effetti avversi dell'incidente.

In caso di minaccia informatica significativa, le entità finanziarie, se del caso, informano i loro clienti potenzialmente interessati in merito alle opportune misure di protezione che i clienti stessi possono prendere in considerazione.

4. Entro i termini da fissare a norma dell'articolo 20, primo comma, lettera a), punto ii), le entità finanziarie trasmettono all'autorità competente interessata:

a) una notifica iniziale;

b) una relazione intermedia dopo la notifica iniziale di cui alla lettera a), non appena lo stato originario dell'incidente cambia in maniera significativa o il trattamento dell'grave incidente TIC cambia alla luce delle nuove informazioni disponibili, seguita, a seconda dei casi, da notifiche aggiornate, ogni qualvolta sia disponibile un aggiornamento della situazione, nonché su specifica richiesta dell'autorità competente;

c) una relazione finale, quando l'analisi delle cause che hanno dato origine all'incidente sia stata completata, indipendentemente dal fatto che le misure di attenuazione siano già state attuate, e quando al posto delle stime siano disponibili i dati dell'impatto effettivo.

5. Ai sensi del presente articolo, le entità finanziarie possono esternalizzare, conformemente al diritto settoriale dell'Unione e nazionale, gli obblighi di segnalazione a un fornitore terzo di servizi. In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di espletare gli obblighi di segnalazione degli incidenti.

6. Dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui al paragrafo 4, l'autorità competente trasmette tempestivamente i dettagli dell'grave incidente TIC ai seguenti destinatari sulla base, ove applicabile, delle rispettive competenze:

a) all'ABE, all'ESMA o all'EIOPA;

b) alla BCE, qualora siano coinvolte le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere a), b) e d);

c) alle autorità competenti, ai punti di contatto unici o ai CSIRT designati o istituiti conformemente alla direttiva (UE) 2022/2555;

d) alle autorità di risoluzione di cui all'articolo 3 della direttiva 2014/59/UE e al Comitato di risoluzione unico (SRB) per quanto riguarda le entità di cui all'articolo 7, paragrafo 2, del regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio ([37]) nonché le entità e i gruppi di cui all'articolo 7, paragrafo 4, lettera b), e all'articolo 7, paragrafo 5, del regolamento (UE) n. 806/2014, qualora tali dettagli riguardino incidenti che comportano un rischio per le funzioni essenziali definite all'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE; e

e) ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale.

7. Una volta ricevute le informazioni conformemente al paragrafo 6, l'ABE, l'ESMA o l'EIOPA e la BCE, in consultazione con l'ENISA e in collaborazione con l'autorità competente interessata, valutano la pertinenza dell'grave incidente TIC rispetto alle autorità competenti in altri Stati membri. A seguito di tale valutazione, l'ABE, l'ESMA o l'EIOPA inviano una notifica al riguardo il prima possibile alle autorità competenti interessate in altri Stati membri. La BCE notifica i membri del Sistema europeo di banche centrali in merito a questioni afferenti il sistema di pagamenti. Sulla base di tale notifica, le autorità competenti adottano, se del caso, tutte le misure necessarie per proteggere l'immediata stabilità del sistema finanziario.

([37]) Regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, del 15 luglio 2014, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010 (GU L 225 del 30.7.2014, pag. 1).

8. La notifica che l'ESMA deve effettuare a norma del paragrafo 7 del presente articolo lascia impregiudicata la responsabilità dell'autorità competente di trasmettere urgentemente i dettagli dell'grave incidente TIC all'autorità pertinente dello Stato membro ospitante, laddove uno dei depositari centrali di titoli svolga una cospicua attività transfrontaliera nello Stato membro ospitante, laddove l'incidente grave connesso alle TIC possa comportare serie conseguenze per i mercati finanziari dello Stato membro ospitante e laddove vi siano accordi di cooperazione tra le autorità competenti in relazione alla vigilanza delle entità finanziarie.

Articolo 20

Armonizzazione dei modelli e dei contenuti per la segnalazione

In consultazione con l'ENISA e la BCE, le AEV, tramite il comitato congiunto, elaborano quanto segue:

a) progetti di norme tecniche di regolamentazione comuni per:

   i) stabilire il contenuto delle segnalazioni relative agli incidenti gravi connessi alle TIC al fine di rispecchiare i criteri di cui all'articolo 18, paragrafo 1, e integrare ulteriori elementi, ad esempio i dettagli per stabilire la rilevanza delle segnalazioni per gli altri Stati membri e se si tratti o meno di un grave incidente operativo o di sicurezza dei pagamenti;

   ii) stabilire i termini della notifica iniziale e di ciascuna relazione di cui all'articolo 19, paragrafo 4;

   iii) stabilire il contenuto della notifica per le minacce informatiche significative.

   All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, in particolare al fine di garantire che, ai fini della lettera a), punto ii) del presente comma, termini differenti possano rispecchiare, se del caso, alcune specificità dei settori finanziari, fatto salvo il mantenimento di un approccio coerente alla segnalazione degli incidenti connessi alle TIC a norma del presente regolamento e della direttiva (UE) 2022/2555. Se del caso, le AEV forniscono una giustificazione quando si discostano dagli approcci adottati nel contesto di tale direttiva;

b) progetti di norme tecniche di attuazione comuni per stabilire i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un grave incidente TIC e notificare una minaccia informatica significativa.

Le AEV trasmettono alla Commissione i progetti di norme tecniche di regolamentazione comuni di cui al primo comma, lettera a), e i progetti di norme tecniche di attuazione comuni di cui al primo comma, lettera b), entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione comuni di cui al primo comma, lettera a), in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

Alla Commissione è conferito il potere di adottare le norme tecniche di attuazione comuni di cui al primo comma, lettera b), in conformità dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 21

Centralizzazione delle segnalazioni di incidenti gravi connessi alle TIC

1. In consultazione con la BCE e l'ENISA, le AEV, tramite il comitato congiunto, redigono una relazione congiunta che valuta la fattibilità dell'ulteriore centralizzazione delle segnalazioni degli incidenti mediante l'istituzione di un polo UE unico per la segnalazione degli incidenti gravi connessi alle TIC da parte delle entità finanziarie. La relazione congiunta esamina i criteri per agevolare il flusso delle segnalazioni di incidenti connessi alle TIC, ridurre i costi associati e corroborare le analisi tematiche per migliorare la convergenza della vigilanza.

2. La relazione congiunta di cui al paragrafo 1 comprende almeno gli elementi seguenti:

a) prerequisiti per l'istituzione di un polo UE unico;

b) benefici, limiti e rischi, compresi i rischi associati all'elevata concentrazione di informazioni sensibili;

c) la necessaria capacità di garantire l'interoperabilità rispetto ad altri sistemi di segnalazione pertinenti;

d) elementi della gestione operativa;

e) condizioni di adesione;

f) modalità tecniche per l'accesso al polo UE unico da parte delle entità finanziarie e le autorità nazionali competenti;

g) una valutazione preliminare dei costi finanziari sostenuti per l'istituzione della piattaforma operativa su cui dovrà fondarsi il polo UE unico, comprese le richieste competenze.

3. Le AEV presentano la relazione di cui al paragrafo 1 al Parlamento europeo, al Consiglio e alla Commissione entro il 17 gennaio 2025.

Articolo 22

Riscontri forniti dalle autorità di vigilanza

1. Fatti salvi il contributo tecnico, la consulenza o i rimedi e il successivo seguito dato che possono essere forniti, ove applicabile, conformemente al diritto nazionale, dai CSIRT ai sensi della direttiva (UE) 2022/2555, l'autorità competente, dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui all'articolo 19, paragrafo 4, ne accusa ricevuta e può, ove fattibile, fornire tempestivamente all'entità finanziaria riscontri pertinenti e proporzionali o orientamenti di alto livello, in particolare rendendo disponibili le informazioni e i dati pertinenti anonimizzati su minacce analoghe, e può discutere rimedi applicati a livello di entità finanziaria e metodi per ridurre al minimo e attenuare gli effetti avversi nel settore finanziario. Fatti salvi i riscontri ricevuti dalle autorità di vigilanza, le entità finanziarie restano pienamente responsabili del trattamento e delle conseguenze degli incidenti connessi alle TIC segnalati a norma dell'articolo 19, paragrafo 1.

2. Le AEV, tramite il comitato congiunto, riferiscono con frequenza annuale, sulla base di dati anonimizzati e aggregati, in merito agli incidenti gravi connessi alle TIC, i cui dettagli sono forniti dalle autorità competenti a norma dell'articolo 19, paragrafo 6, indicando almeno il numero degli incidenti gravi connessi alle TIC, la natura, l'impatto sulle operazioni delle entità finanziarie o dei clienti, i costi sostenuti e le azioni di riparazione adottate.

Le AEV emanano segnalazioni di allerta e redigono statistiche di alto livello a supporto delle valutazioni della vulnerabilità e delle minacce connesse alle TIC.

Articolo 23

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

I requisiti contenuti nel presente capo si applicano anche agli incidenti operativi o relativi alla sicurezza dei pagamenti ovvero ai gravi incidenti operativi o relativi alla sicurezza dei pagamenti allorché riguardano enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica.

CAPO IV

Test di resilienza operativa digitale

Articolo 24

Requisiti generali per lo svolgimento dei test di resilienza operativa digitale

1. Allo scopo di valutare la preparazione alla gestione degli incidenti connessi alle TIC, di identificare punti deboli, carenze e lacune della resilienza operativa digitale e di attuare tempestivamente misure correttive, le entità finanziarie diverse dalle microimprese, tenuto conto dei criteri di cui all'articolo 4, paragrafo 2, stabiliscono, mantengono e riesaminano un programma di test di resilienza operativa digitale solido ed esaustivo quale parte integrante del quadro per la gestione dei rischi informatici di cui all'articolo 6.

2. Il programma di test di resilienza operativa digitale comprende una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare conformemente agli articoli 25 e 26.

3. Nello svolgimento del programma di test di resilienza operativa digitale di cui al paragrafo 1 del presente articolo, le entità finanziarie, diverse dalle microimprese, adottano un approccio basato sul rischio che prende in considerazione i criteri di cui all'articolo 4, paragrafo 2, tenendo debitamente conto del mutevole contesto dei rischi informatici, di eventuali rischi specifici cui l'entità finanziaria interessata è o potrebbe essere esposta, della criticità dei patrimoni informativi e dei servizi forniti, nonché di qualsiasi altro fattore giudicato rilevante dall'entità finanziaria stessa.

4. Le entità finanziarie, diverse dalle microimprese, assicurano che i test siano svolti da soggetti indipendenti, interni o esterni. Se i test sono svolti da un soggetto incaricato dello svolgimento dei test interno, le entità finanziarie dedicano risorse sufficienti e garantiscono che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test.

5. Le entità finanziarie, diverse dalle microimprese, definiscono procedure e politiche per dare un ordine di priorità ai problemi riscontrati durante lo svolgimento dei test, per classificarli e porvi rimedio; stabiliscono inoltre metodologie di convalida interne per accertare che tutti i punti deboli, le carenze o le lacune che sono stati individuati siano pienamente affrontati.

6. Le entità finanziarie, diverse dalle microimprese, provvedono affinché, con cadenza almeno annuale, siano eseguiti test adeguati su tutti i sistemi e le applicazioni di TIC a supporto di funzioni essenziali o importanti.

Articolo 25

Test di strumenti e sistemi di TIC

1. Il programma di test di resilienza operativa digitale di cui all'articolo 24 prevede, conformemente ai criteri di cui all'articolo 4, paragrafo 2, l'esecuzione di test adeguati, tra cui valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test end-to-end e test di penetrazione.

2. I depositari centrali di titoli e le controparti centrali effettuano valutazioni della vulnerabilità prima di ciascun rilascio o nuovo rilascio di nuovi o già esistenti applicazioni e componenti infrastrutturali, e servizi TIC a supporto delle funzioni essenziali o importanti dell'entità finanziaria.

3. Le microimprese eseguono i test di cui al paragrafo 1 combinando un approccio basato sul rischio con una pianificazione strategica dei test relativi alle TIC, tenendo debitamente conto della necessità di mantenere un approccio equilibrato tra l'entità delle risorse e il tempo da assegnare ai test relativi alle TIC di cui al presente articolo, da un lato, e l'urgenza, il tipo di rischio, la criticità dei patrimoni informativi e dei servizi forniti nonché qualsiasi altro fattore rilevante, compresa la capacità dell'entità finanziaria di assumere rischi calcolati, dall'altro.

Articolo 26

Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)

1. Le entità finanziarie, diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese, che sono identificate conformemente al paragrafo 8, terzo comma, del presente articolo, effettuano test avanzati sotto forma di test di penetrazione basati su minacce con cadenza almeno triennale. Sulla base del profilo di rischio dell'entità finanziaria e tenuto conto delle circostanze operative, l'autorità competente può, se necessario, chiedere all'entità finanziaria di ridurre o aumentare tale frequenza.

2. Ciascun test di penetrazione guidato dalla minaccia riguarda alcune o tutte le funzioni essenziali o importanti dell'entità finanziaria ed è effettuato sui sistemi attivi di produzione a supporto di tali funzioni.

Le entità finanziarie identificano tutti i sistemi, i processi e le tecnologie TIC sottostanti a supporto delle funzioni essenziali o importanti e tutti i pertinenti servizi TIC, compresi quelli a supporto di funzioni essenziali o importanti che sono stati esternalizzate o appaltate a fornitori terzi di servizi TIC.

Le entità finanziarie valutano quali funzioni essenziali o importanti debbano essere interessate dai TLPT. Il risultato della valutazione determina il preciso ambito di applicazione dei TLPT ed è convalidato dalle autorità competenti.

3. Qualora i fornitori terzi di servizi TIC rientrino nell'ambito di applicazione dei TLPT, l'entità finanziaria adotta le misure e le salvaguardie necessarie per garantire la partecipazione di tali fornitori terzi di servizi TIC ai TLPT ed è sempre pienamente responsabile di garantire il rispetto del presente regolamento.

4. Fatto salvo il paragrafo 2, primo e secondo comma, laddove si ritiene ragionevolmente che la partecipazione di un fornitore terzo di servizi TIC ai TLPT di cui al paragrafo 3 possa avere un impatto avverso sulla qualità o la sicurezza dei servizi offerti dal fornitore terzo di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento, ovvero sulla riservatezza dei dati relativi a tali servizi, l'entità finanziaria e il fornitore terzo di servizi TIC possono concordare per iscritto che il fornitore terzo di servizi TIC stipuli direttamente accordi contrattuali con un soggetto incaricato dello svolgimento dei test esterno, allo scopo di condurre, sotto la direzione di un'entità finanziaria designata, un TLPT congiunto che coinvolga diverse entità finanziarie (*pooled testing*) a cui il fornitore terzo di servizi TIC fornisce tali servizi.

Detto test congiunto riguarda la pertinente gamma di servizi TIC a supporto delle funzioni essenziali o importanti appaltate dalle entità finanziarie al rispettivo fornitore terzo di servizi TIC. I test congiunti sono considerati TLPT effettuati dalle entità finanziarie che partecipano ai test congiunti.

Il numero di entità finanziarie che partecipano ai test congiunti è debitamente calibrato tenendo conto della complessità e dei tipi di servizi interessati.

5. Le entità finanziarie, cooperando con i fornitori terzi di servizi TIC e altre parti coinvolte, inclusi i soggetti incaricati dello svolgimento dei test ma escluse le autorità competenti, applicano efficaci controlli di gestione del rischio per attenuare i rischi di potenziali impatti sui dati, danni alle attività e perturbazioni delle funzioni essenziali o importanti, delle operazioni o dei servizi delle entità finanziarie, delle loro controparti o del settore finanziario.

6. Alla fine dei test, dopo che le relazioni e i piani correttivi siano stati concordati, l'entità finanziaria e, ove applicabile, i soggetti incaricato dello svolgimento dei test esterni trasmettono all'autorità, designata conformemente al paragrafo 9 o 10, una sintesi delle pertinenti risultanze, i piani correttivi e la documentazione attestante che i TLPT sono stati svolti conformemente ai requisiti.

7. Le autorità forniscono alle entità finanziarie un attestato che conferma che i test sono stati svolti conformemente ai requisiti, come si evince dalla documentazione, in modo da consentire il riconoscimento reciproco dei TLPT tra le autorità competenti. L'entità finanziaria notifica all'autorità competente interessata l'attestato, la sintesi delle pertinenti risultanze e i piani correttivi.

Fatto salvo tale attestato, le entità finanziarie rimangono sempre pienamente responsabili degli impatti dei test di cui al paragrafo 4.

8. Per l'effettuazione dei TLPT, le entità finanziarie si avvalgono di soggetti incaricati dello svolgimento dei test in conformità dell'articolo 27. Quando ricorrono a soggetti incaricati dello svolgimento dei test interni per l'effettuazione di TLPT, le entità finanziarie si avvalgono di un soggetto incaricato dello svolgimento dei test esterno ogni tre test.

Gli enti creditizi classificati come significativi a norma dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013, ricorrono esclusivamente a soggetto incaricato dello svolgimento dei test esterni conformemente all'articolo 27, paragrafo 1, lettere da a) a e).

Le autorità competenti identificano le entità finanziarie che hanno l'obbligo di svolgere TLPT tenendo conto dei criteri di cui all'articolo 4, paragrafo 2, sulla base della valutazione degli elementi seguenti:

a) i fattori correlati all'impatto, in particolare la portata dell'impatto sul settore finanziario dei servizi forniti e delle attività svolte dall'entità finanziaria;

b) i possibili problemi di stabilità finanziaria, tra cui il carattere sistemico dell'entità finanziaria a livello di Unione o nazionale, a seconda dei casi;

c) lo specifico profilo dei rischi informatici, il livello di maturità delle TIC dell'entità finanziaria o le caratteristiche tecnologiche in questione.

9. Gli Stati membri possono designare un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT nel settore finanziario a livello nazionale e le affidano tutte le competenze e tutti i compiti a tal fine.

10. In assenza di una designazione a norma del paragrafo 9 del presente articolo e fatto salvo il potere di identificare le entità finanziarie tenute a svolgere TLPT, un'autorità competente può delegare l'esercizio di alcuni o di tutti i compiti di cui al presente articolo e all'articolo 27 a un'altra autorità nazionale nel settore finanziario.

11. Di concerto con la BCE, le AEV elaborano progetti di norme tecniche di regolamentazione comuni conformemente al quadro di riferimento TIBER-EU al fine di specificare ulteriormente quanto segue:

a) i criteri utilizzati ai fini dell'applicazione del paragrafo 8, secondo comma;

b) i requisiti e le norme che disciplinano il ricorso a soggetto incaricato dello svolgimento dei test interni;

c) i requisiti concernenti:

   i) l'ambito dei TLPT di cui al paragrafo 2;

   ii) l'approccio e la metodologia da seguire per i test in ciascuna fase del relativo processo;

   iii) i risultati, la chiusura e le fasi correttive dei test;

d) il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco di tali test, nel contesto di entità finanziarie che operano in più di uno Stato membro, al fine di consentire un livello adeguato di partecipazione alla vigilanza, nonché un'attuazione flessibile per tener conto delle specificità dei sottosettori finanziari o dei mercati finanziari locali.

All' atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono debitamente conto di eventuali caratteristiche specifiche derivanti dalla natura distinta delle attività nei diversi settori dei servizi finanziari.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

Articolo 27

Requisiti per i soggetti incaricati dello svolgimento dei test per lo svolgimento dei TLPT

1. Per lo svolgimento dei test di penetrazione basati su minacce, le entità finanziarie ricorrono unicamente a soggetto incaricato dello svolgimento dei test che:

a) possano vantare il più alto grado di idoneità e reputazione;

b) possiedano capacità tecniche e organizzative e dimostrino esperienza specifica nel campo delle analisi delle minacce, dei test di penetrazione e dei test red team;

c) siano certificati da un ente di accreditamento in uno Stato membro o rispettino codici formali di condotta o quadri etici;

d) forniscano una garanzia indipendente o una relazione di audit concernente la solida gestione dei rischi derivanti dallo svolgimento di TLPT, comprese la dovuta protezione delle informazioni riservate dell'entità finanziaria e il risarcimento dei rischi commerciali dell'entità finanziaria;

e) siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza.

2. Quando ricorrono a soggetto incaricato dello svolgimento dei test interni, le entità finanziare devono provvedere affinché, oltre all'obbligo di cui al paragrafo 1, siano soddisfatte le condizioni seguenti:

a) tale ricorso è stato approvato dall'autorità competente interessata o dall'autorità pubblica unica designata conformemente all'articolo 26, paragrafi 9 e 10;

b) l'autorità competente interessata ha verificato che l'entità finanziaria dispone di risorse dedicate sufficienti e che essa ha garantito che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test; e

c) il soggetto che fornisce analisi delle minacce è esterno all'entità finanziaria.

3. Le entità finanziarie garantiscono che i contratti conclusi con i soggetti incaricati dello svolgimento dei test esterni prevedano una solida gestione dei risultati dei TLPT e che qualsiasi trattamento dei dati, comprese la generazione, la conservazione, l'aggregazione, l'elaborazione, la segnalazione, la comunicazione o la distruzione, non comporti rischi per l'entità finanziaria.

CAPO V

Gestione dei rischi informatici derivanti da terzi

Sezione I

Principi fondamentali di una solida gestione dei rischi informatici derivanti da terzi

Articolo 28

Principi generali

1. Le entità finanziarie gestiscono i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi di cui all'articolo 6, paragrafo 1, e conformemente ai principi indicati di seguito:

a) le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla normativa applicabile in materia di servizi finanziari;

b) la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie si svolge nel rispetto del principio di proporzionalità, tenendo conto:

i) della natura, della portata, della complessità e dell'importanza delle dipendenze connesse alle TIC;

ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la disponibilità delle attività e dei servizi finanziari a livello individuale e di gruppo.

2. Nel contesto del quadro per la gestione dei rischi informatici TIC, le entità finanziarie diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese adottano e riesaminano periodicamente una strategia per i rischi informatici derivanti da terzi, tenendo conto della strategia basata su una varietà di fornitori di cui all'articolo 6, paragrafo 9, ove applicabile. Tale strategia comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi e si applica su base individuale e, se del caso, su base subconsolidata e consolidata. Sulla base di una valutazione del profilo di rischio complessivo dell'entità finanziaria e della portata e della complessità dei servizi operativi, l'organo di gestione riesamina periodicamente i rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti.

3. Nel contesto del quadro per la gestione dei rischi informatici, le entità finanziarie mantengono e aggiornano a livello di entità, e su base subconsolidata e consolidata, un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi.

Gli accordi contrattuali di cui al primo comma sono opportunamente documentati, distinguendo quelli che si riferiscono a servizi TIC a supporto di funzioni essenziali o importanti dagli altri.

Le entità finanziarie comunicano almeno una volta all'anno alle autorità competenti il numero di nuovi accordi per l'utilizzo di servizi TIC, le categorie di fornitori terzi di servizi TIC, il tipo di accordi contrattuali e le funzioni e i servizi TIC forniti.

Su richiesta, le entità finanziarie mettono a disposizione dell'autorità competente il registro delle informazioni completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

Le entità finanziarie informano tempestivamente l'autorità competente in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti, nonché del momento in cui una funzione diventa essenziale o importante.

4. Prima di stipulare un accordo contrattuale per l'utilizzo di servizi TIC, le entità finanziarie:

a) valutano se l'accordo contrattuale riguardi l'utilizzo di servizi TIC a supporto di una funzione essenziale o importante;

b) verificano se siano soddisfatte le condizioni di vigilanza per la conclusione del contratto;

c) identificano e valutano tutti i rischi pertinenti relativi all'accordo contrattuale, compresa la possibilità che tale accordo contrattuale possa aggravare il rischio di concentrazione delle TIC di cui all'articolo 29;

d) effettuano controlli di dovuta diligenza (*due diligence*) sui potenziali fornitori terzi di servizi TIC e ne garantiscono l'idoneità lungo tutto il processo di selezione e valutazione;

e) individuano e valutano i conflitti d'interessi che possano derivare dall'accordo contrattuale.

5. Le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi TIC che soddisfano standard appropriati in materia di sicurezza delle informazioni. Laddove tali accordi contrattuali riguardino funzioni essenziali o importanti, le entità finanziarie, prima di concludere detti accordi, prendono in debita considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli standard di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni.

6. Nell'esercizio dei diritti di accesso, ispezione e audit nei confronti del fornitore terzo di servizi TIC, le entità finanziarie predeterminano, sulla base di un approccio basato sul rischio, la frequenza delle verifiche di audit e delle ispezioni nonché i settori da sottoporre ad audit, aderendo a standard di audit comunemente accettate in conformità di eventuali indicazioni di vigilanza sull'uso e l'integrazione di tali standard di audit.

Laddove gli accordi contrattuali conclusi con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, l'entità finanziaria verifica che i revisori, indipendentemente dal fatto che siano revisori interni o esterni o siano un gruppo di revisori, possiedano competenze e conoscenze adeguate per svolgere efficacemente gli audit e le valutazioni del caso.

7. Le entità finanziarie stabiliscono clausole che consentano la risoluzione degli accordi contrattuali per l'utilizzo di servizi TIC in una qualsiasi delle circostanze seguenti:

a) rilevante violazione, da parte del fornitore terzo di servizi TIC, di leggi, regolamenti o condizioni contrattuali applicabili;

b) circostanze, identificate nel corso del monitoraggio dei rischi informatici derivanti da terzi, ritenute suscettibili di alterare l'esercizio delle funzioni previsto a norma dell'accordo contrattuale, tra cui modifiche di rilievo che incidano sull'accordo o sulla situazione del fornitore terzo di servizi TIC;

c) punti deboli del fornitore terzo di servizi TIC emersi riguardo alla sua gestione complessiva dei rischi informatici e, in particolare, nel modo in cui il fornitore garantisce la disponibilità, autenticità, integrità e riservatezza dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali;

d) laddove l'autorità competente non sia più in grado di vigilare efficacemente sull'entità finanziaria per via delle condizioni dell'accordo contrattuale in questione o delle circostanze ivi afferenti.

8. Per i servizi TIC a supporto di funzioni essenziali o importanti, le entità finanziarie predispongono strategie di uscita. Tali strategie tengono conto dei rischi che possono emergere a livello dei fornitori terzi di servizi TIC, in particolare possibili disfunzioni dei fornitori stessi, il deterioramento della qualità dei servizi TIC forniti, una perturbazione dell'attività commerciale conseguente a una fornitura di servizi TIC inadeguata o carente, oppure gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio del rispettivo servizio TIC oppure la risoluzione di accordi contrattuali con fornitori terzi di servizi TIC in una delle circostanze di cui al paragrafo 7.

Le entità finanziarie garantiscono di poter porre termine agli accordi contrattuali senza:

a) perturbare le proprie attività commerciali;

b) limitare il rispetto dei requisiti normativi;

c) pregiudicare la continuità e la qualità dei servizi forniti ai clienti.

I piani di uscita sono esaustivi, documentati e, conformemente ai criteri di cui all'articolo 4, paragrafo 2, sottoposti a test adeguati e riesaminati periodicamente.

Le entità finanziarie identificano soluzioni alternative ed elaborano piani di transizione che consentano loro di trasferire i servizi TIC previsti dal contratto e i relativi dati dal fornitore terzo di servizi TIC, in maniera sicura e nella loro interezza, a fornitori alternativi oppure reintegrarli al proprio interno.

Le entità finanziarie dispongono di misure di emergenza idonee per mantenere la continuità operativa qualora si verifichino le circostanze di cui al primo comma.

9. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di attuazione per definire modelli standard in relazione al registro delle informazioni di cui al paragrafo 3, comprese le informazioni comuni a tutti gli accordi contrattuali per l'utilizzo di servizi TIC. Le AEV presentano tali progetti di norme tecniche di attuazione alla Commissione entro il 17 gennaio 2024.

Alla Commissione è conferito il potere di adottare le norme tecniche di attuazione di cui al primo comma in conformità dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

10. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per precisare ulteriormente il contenuto dettagliato della politica di cui al paragrafo 2, in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni. Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

Articolo 29

Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità

1. All'atto dell'identificazione e della valutazione dei rischi di cui all'articolo 28, paragrafo 4, lettera c), le entità finanziarie tengono conto altresì dell'eventualità che la prevista conclusione di un accordo contrattuale relativo a servizi TIC a supporto di funzioni essenziali o importanti possa avere una delle seguenti conseguenze:

a) la conclusione di un contratto con un fornitore terzo di servizi TIC non facilmente sostituibile; o

b) la presenza di molteplici accordi contrattuali relativi alla prestazione di servizi TIC a supporto di funzioni essenziali o importanti con lo stesso fornitore terzo oppure con fornitori terzi strettamente connessi.

Le entità finanziarie vagliano i benefici e i costi di soluzioni alternative, quali il ricorso a diversi fornitori terzi di servizi TIC, verificando se e come le soluzioni previste soddisfino le esigenze commerciali e consentano di conseguire gli obiettivi fissati nella propria strategia di resilienza digitale.

2. Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano la possibilità che un fornitore terzo di servizi TIC subappalti a sua volta servizi TIC a supporto di una funzione essenziale o importante ad altri fornitori terzi di servizi TIC, le entità finanziarie vagliano i benefici e i rischi che possono derivare da tale subappalto, in particolare nel caso di un subappaltatore di TIC stabilito in un paese terzo.

Qualora gli accordi contrattuali riguardino servizi TIC a supporto delle funzioni essenziali o importanti, le entità finanziarie tengono in debita considerazione le disposizioni del diritto fallimentare applicabili in caso di fallimento del fornitore terzo di servizi TIC come pure eventuali restrizioni relative all'urgente ripristino dei dati dell'entità finanziaria.

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti siano conclusi con un fornitore terzo di servizi TIC stabilito in un paese terzo, le entità finanziarie, in aggiunta alle considerazioni di cui al secondo comma, tengono conto altresì del rispetto delle norme dell'UE sulla protezione dei dati e dell'effettiva applicazione della legge in tale paese terzo.

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano un subappalto, le entità finanziarie valutano se e come catene di subappalti potenzialmente lunghe e complesse possano incidere sulla loro capacità di monitorare pienamente le funzioni appaltate e sulla capacità dell'autorità competente di vigilare efficacemente, a tal proposito, sull'entità finanziaria.

Articolo 30

Principali disposizioni contrattuali

1. I diritti e gli obblighi dell'entità finanziaria e del fornitore terzo di servizi TIC sono attribuiti chiaramente e definiti per iscritto. Il testo integrale del contratto comprende gli accordi sul livello dei servizi ed è contenuto in un documento scritto disponibile alle parti in formato cartaceo oppure in un documento in altro formato scaricabile, durevole e accessibile.

2. Gli accordi contrattuali per l'utilizzo di servizi TIC comprendono almeno gli elementi seguenti:

a) la descrizione chiara e completa di tutte le funzioni che il fornitore terzo di servizi TIC deve svolgere e tutti i servizi TIC che deve prestare, comprese l'indicazione dell'eventuale autorizzazione a subappaltare un servizio TIC a sostegno di una funzione essenziale o importante o parti significative di essa e, in caso affermativo, le condizioni di tale subappalto;

b) le località, segnatamente le regioni o i paesi, in cui si devono svolgere le funzioni e prestare i servizi TIC appaltati o subappaltati e in cui si devono trattare i dati, compreso il luogo di conservazione, nonché l'obbligo, per il fornitore terzo di servizi TIC, di segnalare in anticipo all'entità finanziaria l'intenzione di cambiare tale o tali località;

c) le disposizioni in materia di disponibilità, autenticità, integrità e riservatezza in relazione alla protezione dei dati, compresi i dati personali;

d) le disposizioni relative alle garanzie di accesso, ripristino e restituzione, in un formato facilmente accessibile, di dati personali e non personali trattati dall'entità finanziaria in caso di insolvenza, risoluzione o interruzione delle operazioni commerciali del fornitore terzo di servizi TIC o in caso di risoluzione degli accordi commerciali;

e) le descrizioni dei livelli di servizio, compresi relativi aggiornamenti e revisioni;

f) l'obbligo per il fornitore terzo di servizi TIC di prestare assistenza all'entità finanziaria senza costi aggiuntivi o a un costo stabilito ex ante, qualora si verifichi un incidente connesso alle TIC relativo al servizio TIC fornito all'entità finanziaria;

g) l'obbligo per il fornitore terzo di servizi di TIC di operare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria, comprese le persone da queste nominate;

h) i diritti di risoluzione e il relativo termine minimo di preavviso per la risoluzione degli accordi contrattuali, conformemente alle attese delle autorità competenti e delle autorità di risoluzione;

i) le condizioni riguardanti la partecipazione dei fornitori terzi di servizi TIC ai programmi di sensibilizzazione sulla sicurezza delle TIC e alle attività di formazione sulla resilienza operativa digitale delle entità finanziarie conformemente all'articolo 13, paragrafo 6.

3. Gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti comprendono, in aggiunta agli elementi di cui al paragrafo 2, almeno quanto segue:

a) la descrizione completa dei livelli di servizio, comprendente i relativi aggiornamenti e revisioni con precisi obiettivi quantitativi e qualitativi, in termini di prestazioni, nell'ambito dei livelli di servizio concordati, in modo da consentire un monitoraggio efficace da parte dell'entità finanziaria dei servizi TIC e l'applicazione, senza indebito ritardo, di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati;

b) termini di preavviso e obblighi di segnalazione per il fornitore terzo di servizi TIC nei confronti dell'entità finanziaria, tra cui la notifica di eventuali sviluppi che potrebbero esercitare un impatto significativo sulla capacità del fornitore terzo di servizi TIC di prestare servizi a supporto di funzioni essenziali o importanti efficacemente, in linea con i livelli di servizio concordati;

c) l'obbligo per il fornitore terzo di servizi TIC di attuare e testare i piani operativi d'emergenza e di predisporre misure, strumenti e politiche per la sicurezza delle TIC che offrano un adeguato livello di sicurezza per la fornitura dei servizi da parte dell'entità finanziaria, in linea con il proprio quadro normativo;

d) l'obbligo per il fornitore terzo di servizi TIC di partecipare e cooperare pienamente al TLPT dell'entità finanziaria di cui agli articoli 26 e 27;

e) il diritto di monitorare costantemente le prestazioni del fornitore terzo di servizi TIC, che comporta quanto segue:

i) diritti incondizionati di accesso, ispezione e audit da parte dell'entità finanziaria — o di un terzo designato a tal fine — e dell'autorità competente nonché il diritto di ottenere copia della documentazione pertinente in loco, se di importanza critica per le operazioni del fornitore terzo di servizi TIC, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione;

ii) il diritto di concordare livelli di garanzia alternativi, qualora siano interessati i diritti di altri clienti;

iii) l'obbligo per il fornitore terzo di servizi TIC di cooperare senza riserve nel corso delle ispezioni e degli audit in loco svolti dalle autorità competenti, dall'autorità di sorveglianza capofila, dall'entità finanziaria o da un terzo designato; e

iv) l'obbligo di fornire dettagli sull'ambito di applicazione, sulle procedure da seguire e sulla frequenza di tali ispezioni e audit;

f) le strategie di uscita, in particolare la definizione di un adeguato periodo di transizione obbligatorio:

i) durante il quale il fornitore terzo di servizi TIC continuerà a prestare i suoi servizi TIC o a esercitare le sue funzioni allo scopo di ridurre il rischio di perturbazioni presso l'entità finanziaria o di garantire la sua efficace risoluzione e ristrutturazione;

ii) che permetta all'entità finanziaria di migrare verso un altro fornitore terzo di servizi TIC oppure di adottare soluzioni interne coerenti con la complessità del servizio prestato.

In deroga alla lettera e), il fornitore terzo di servizi TIC e l'entità finanziaria che è una microimpresa possono convenire che i diritti di accesso, ispezione e audit dell'entità finanziaria possano essere delegati a un terzo indipendente, nominato dal fornitore terzo di servizi TIC, e che l'entità finanziaria possa richiedere in qualsiasi momento al terzo informazioni e garanzie sulle prestazioni del fornitore terzo di servizi TIC.

4. All'atto della negoziazione degli accordi contrattuali, le entità finanziarie e i fornitori terzi di servizi TIC prendono in considerazione il ricorso a clausole contrattuali standard elaborate dalle autorità pubbliche per servizi specifici.

5. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente gli elementi di cui al paragrafo 2, lettera a), che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

Sezione II

Quadro di sorveglianza dei fornitori terzi critici di servizi TIC

Articolo 31

Designazione dei fornitori terzi critici di servizi TIC

1. Le AEV, tramite il comitato congiunto e su raccomandazione del forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1:

a) designano i fornitori terzi di servizi TIC che sono critici per le entità finanziarie, a seguito di una valutazione che tiene conto dei criteri di cui al paragrafo 2;

b) nominano quale autorità di sorveglianza capofila di ciascun fornitore terzo critico di servizi TIC la AEV che è responsabile, a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, delle entità finanziarie che possiedono complessivamente la quota maggiore delle attività totali rispetto al valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del pertinente fornitore terzo critico di servizi TIC, secondo quanto risulta dalla somma dei singoli bilanci di quelle entità finanziarie.

2. La designazione di cui al paragrafo 1, lettera a), si fonda su tutti i criteri indicati di seguito in relazione ai servizi TIC prestati da un fornitore terzo di servizi TIC:

a) l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari qualora il fornitore terzo di servizi TIC pertinente sia interessato da una disfunzione operativa su vasta scala che gli impedisca di fornire i suoi servizi, tenendo conto del numero di entità finanziarie e del valore totale delle attività delle entità finanziarie cui quel fornitore terzo di servizi TIC presta servizi;

b) il carattere sistemico o l'importanza delle entità finanziarie che dipendono da quel fornitore terzo di servizi TIC, valutati in conformità dei parametri seguenti:

   i) il numero di enti a rilevanza sistemica a livello globale (G-SII) o di altri enti a rilevanza sistemica (O-SII) che dipendono dal rispettivo fornitore terzo di servizi TIC;

   ii) l'interdipendenza tra i G-SII o gli O-SII di cui al punto i) e altre entità finanziarie, comprese le situazioni in cui i G-SII o gli O-SII prestano servizi finanziari infrastrutturali ad altre entità finanziarie;

c) la dipendenza delle entità finanziarie dai servizi prestati dal pertinente fornitore terzo di servizi TIC in rapporto alle funzioni essenziali o importanti delle entità finanziarie che in ultima analisi coinvolgono quel medesimo fornitore terzo di servizi TIC, indipendentemente dal fatto che le entità finanziarie dipendano da tali servizi direttamente o indirettamente, mediante accordi di subappalto;

d) il grado di sostituibilità del fornitore terzo di servizi TIC, prendendo in considerazione i parametri seguenti:

   i) la mancanza di alternative reali, anche parziali, dovuta al limitato numero di fornitori terzi di servizi TIC attivi su un mercato specifico, alla quota di mercato del fornitore terzo di servizi TIC in questione, o ancora alla complessità tecnica o al grado di sofisticazione, anche in relazione a eventuali tecnologie proprietarie, o alle caratteristiche specifiche dell'organizzazione o dell'attività del fornitore terzo di servizi TIC;

   ii) difficoltà inerenti alla migrazione, totale o parziale, dei dati e dei carichi di lavoro dal fornitore terzo di servizi TIC pertinente a un altro, a causa dei cospicui costi finanziari, del tempo o di altre risorse che possono essere necessarie per il processo di migrazione, oppure dei maggiori rischi informatici o di altri rischi operativi cui l'entità finanziaria può esporsi a causa di tale migrazione.

3. Laddove il fornitore terzo di servizi TIC appartenga a un gruppo, i criteri di cui al paragrafo 2 sono presi in considerazione in relazione ai servizi TIC prestati dal gruppo nel suo insieme.

4. I fornitori terzi critici di servizi TIC che fanno parte di un gruppo designano una persona giuridica come punto di coordinamento per garantire un'adeguata rappresentanza e la comunicazione con l'autorità di sorveglianza capofila.

5. L'autorità di sorveglianza capofila informa il fornitore terzo di servizi TIC in merito all'esito della valutazione che ha portato alla designazione di cui al paragrafo 1, lettera a). Entro sei settimane dalla data della notifica, il fornitore terzo di servizi TIC può presentare all'autorità di sorveglianza capofila una dichiarazione motivata contenente tutte le informazioni pertinenti ai fini della valutazione. L'autorità di sorveglianza capofila esamina la dichiarazione motivata e può richiedere ulteriori informazioni da presentare entro 30 giorni di calendario dal ricevimento di detta dichiarazione.

Dopo aver designato un fornitore terzo di servizi TIC come critico, le AEV, tramite il comitato congiunto, notificano al fornitore terzo di servizi TIC tale designazione e la data di inizio a partire dalla quale sarà effettivamente soggetto ad attività di sorveglianza. La data di inizio è fissata a non più di un mese dall'avvenuta notifica. Il fornitore terzo di servizi TIC notifica alle entità finanziarie a cui presta servizi la propria designazione come critico.

6. Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 57, per integrare il presente regolamento specificando ulteriormente i criteri di cui al paragrafo 2 del presente articolo, entro il 17 luglio 2024.

7. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non è utilizzato fino a quando la Commissione non abbia adottato un atto delegato in conformità del paragrafo 6.

8. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non si applica:

i) alle entità finanziarie che forniscono servizi TIC ad altre entità finanziarie;

ii) ai fornitori terzi di servizi TIC che sono soggetti a quadri di sorveglianza istituiti a supporto dei compiti di cui all'articolo 127, paragrafo 2, del trattato sul funzionamento dell'Unione europea;

iii) ai fornitori intragruppo di servizi TIC;

iv) ai fornitori terzi di servizi TIC che prestano servizi TIC unicamente in uno Stato membro a entità finanziarie attive solo in tale Stato membro.

9. Le AEV, tramite il comitato congiunto, redigono, pubblicano e aggiornano ogni anno l'elenco dei fornitori terzi critici di servizi TIC a livello di Unione.

10. Ai fini del paragrafo 1, lettera a), le autorità competenti, con cadenza annuale e in forma aggregata, trasmettono le relazioni di cui all'articolo 28, paragrafo 3, terzo comma, al forum di sorveglianza istituito ai sensi dell'articolo 32. Il forum di sorveglianza valuta la dipendenza delle entità finanziarie da terzi nel settore delle TIC sulla base delle informazioni ricevute dalle autorità competenti.

11. I fornitori terzi di servizi TIC che non sono inseriti nell'elenco di cui al paragrafo 9 possono chiedere di essere designati come critici conformemente al paragrafo 1, lettera a).

Ai fini del primo comma, il fornitore terzo di servizi TIC presenta una domanda motivata all'ABE, all'ESMA o all'EIOPA; queste ultime, tramite il comitato congiunto, decidono se designare tale fornitore terzo di servizi TIC come critico conformemente al paragrafo 1, lettera a).

La decisione di cui al secondo comma è adottata e notificata al fornitore terzo di servizi TIC entro sei mesi dalla data in cui è stata ricevuta la domanda.

12. Le entità finanziarie ricorrono ai servizi di un fornitore terzo di servizi TIC stabilito in un paese terzo e che è stato designato come critico conformemente al paragrafo 1, lettera a), soltanto se detto fornitore ha istituito un'impresa figlia nell'Unione entro 12 mesi dalla designazione.

13. Il fornitore terzo critico di servizi TIC di cui al paragrafo 12 notifica all'autorità di sorveglianza capofila eventuali cambiamenti nella struttura gestionale dell'impresa figlia istituita nell'Unione.

Articolo 32

Struttura del quadro di sorveglianza

1. Il comitato congiunto, in conformità dell'articolo 57, paragrafo 1, dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, istituisce il forum di sorveglianza come sottocomitato incaricato di coadiuvare il lavoro del comitato congiunto e dell'autorità di sorveglianza capofila di cui all'articolo 31, paragrafo 1, lettera b), per quanto concerne i rischi informatici derivanti da terzi in tutti i settori finanziari. Il forum di sorveglianza prepara i progetti di posizioni comuni e atti comuni del comitato congiunto in tale ambito.

Il forum di sorveglianza discute periodicamente gli sviluppi rilevanti in materia di vulnerabilità e rischi relativi alle TIC e promuove un approccio coerente al monitoraggio dei rischi informatici derivanti da terzi a livello dell'Unione.

2. Il forum di sorveglianza intraprende, con cadenza annuale, una valutazione collettiva degli esiti e delle risultanze delle attività di sorveglianza condotte su tutti i fornitori terzi critici di servizi TIC e promuove misure di coordinamento per potenziare la resilienza operativa digitale delle entità finanziarie, favorire le migliori prassi per contrastare il rischio di concentrazione delle TIC e studiare metodi per attenuare i trasferimenti intersettoriali dei rischi.

3. Il forum di sorveglianza sottopone al comitato congiunto parametri di riferimento generali ai fornitori terzi critici di servizi TIC affinché siano adottati come posizioni congiunte delle AEV ai sensi dell'articolo 56, paragrafo 1, dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

4. Il forum di sorveglianza è composto da:

a) i presidenti delle AEV;

b) un rappresentante di alto livello del personale in servizio dell'autorità competente interessata di cui all'articolo 46 di ciascuno Stato membro;

c) i direttori esecutivi di ciascuna AEV e un rappresentante della Commissione, del CERS, della BCE e dell'ENISA in qualità di osservatori;

d) se del caso, un rappresentante supplementare di un'autorità competente di cui all'articolo 46 di ciascuno Stato membro in qualità di osservatore;

e) ove applicabile, un rappresentante delle autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 responsabile della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come un fornitore terzo di servizi TIC critici in qualità di osservatore.

Il forum di sorveglianza può, se del caso, chiedere il parere di esperti indipendenti nominati a norma del paragrafo 6.

5. Ciascuno Stato membro designa l'autorità competente interessata il cui membro del personale è il rappresentante di alto livello di cui al paragrafo 4, primo comma, lettera b), e ne informa l'autorità di sorveglianza capofila.

Le AEV pubblicano sul loro sito web l'elenco dei rappresentanti di alto livello dell'attuale personale della pertinente autorità competente designati dagli Stati membri.

6. Gli esperti indipendenti di cui al paragrafo 4, secondo comma, sono nominati dal forum di sorveglianza e provengono da un gruppo di esperti selezionati al termine di una procedura di candidatura pubblica e trasparente. Gli esperti indipendenti sono nominati sulla base dell'esperienza maturata in settori quali la stabilità finanziaria, la resilienza operativa digitale e le questioni di sicurezza delle TIC.

Agiscono in piena indipendenza e obiettività nell'interesse esclusivo dell'Unione nel suo insieme, senza chiedere né ricevere istruzioni da parte di istituzioni od organi dell'Unione, governi degli Stati membri o altri soggetti pubblici o privati.

7. Ai sensi dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV, entro il 17 luglio 2024, formulano, ai fini della presente sezione, orientamenti sulla cooperazione tra le AEV e le autorità competenti concernenti le procedure e le condizioni dettagliate per la ripartizione e l'esecuzione dei compiti tra le autorità competenti e le AEV, nonché forniscono dettagli sugli scambi di informazioni necessari alle autorità competenti per garantire il seguito da dare alle raccomandazioni a norma dell'articolo 35, paragrafo 1, lettera d) rivolte ai fornitori terzi critici di servizi TIC.

8. I requisiti di cui alla presente sezione non pregiudicano l'applicazione della direttiva (UE) 2022/2555 né di altre norme dell'Unione in materia di sorveglianza applicabili ai fornitori di servizi di cloud computing.

9. Sulla base di un lavoro preparatorio svolto dal forum di sorveglianza, le AEV, tramite il comitato congiunto, trasmettono ogni anno una relazione sull'applicazione della presente sezione al Parlamento europeo, al Consiglio e alla Commissione.

Articolo 33

Compiti dell'autorità di sorveglianza capofila

1. L'autorità di sorveglianza capofila, nominata conformemente all'articolo 31, paragrafo 1, lettera b), effettua la sorveglianza dei fornitori terzi critici di servizi TIC assegnati e, ai fini di tutte le questioni relative alla sorveglianza, è il principale punto di contatto per tali fornitori terzi critici di servizi TIC.

2. Ai fini del paragrafo 1, l'autorità di sorveglianza capofila valuta se ciascun fornitore terzo critico di servizi TIC abbia predisposto norme, procedure, meccanismi e accordi esaustivi, solidi ed efficaci per gestire i rischi informatici cui esso può esporre le entità finanziarie.

La valutazione di cui al primo comma si concentra principalmente sui servizi TIC forniti dal fornitore terzo critico di servizi TIC a supporto di funzioni essenziali o importanti delle entità finanziarie. Se necessario per affrontare tutti i rischi pertinenti, tale valutazione si estende ai servizi TIC a supporto di funzioni diverse da quelle essenziali o importanti.

3. La valutazione di cui al paragrafo 2 riguarda:

a) requisiti in materia di TIC atti a garantire, in particolare, la sicurezza, la disponibilità, la continuità, la scalabilità e la qualità dei servizi che il fornitore terzo critico di servizi TIC presta alle entità finanziarie, nonché la capacità di mantenere standard di, disponibilità, autenticità, integrità o riservatezza dei dati costantemente elevati;

b) la sicurezza fisica che contribuisce a mantenere la sicurezza delle TIC, compresa la sicurezza dei locali, delle attrezzature e dei centri di elaborazione dati;

c) i processi di gestione del rischio, comprese le politiche di gestione dei rischi informatici, la politica di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC;

d) i meccanismi di governance, compresa una struttura organizzativa dotata di linee e norme in materia di responsabilità chiare, trasparenti e coerenti che consentano un'efficace gestione dei rischi informatici;

e) l'identificazione, il monitoraggio e la tempestiva segnalazione alle entità finanziarie di incidenti significativi connessi alle TIC, la gestione e la risoluzione di tali incidenti, in particolare degli attacchi informatici;

f) i meccanismi per la portabilità dei dati, la portabilità e l'interoperabilità delle applicazioni, per assicurare un effettivo esercizio dei diritti di risoluzione da parte delle entità finanziarie;

g) i test su sistemi, infrastrutture e controlli relativi alle TIC;

h) gli audit in materia di TIC;

i) l'utilizzo dei pertinenti standard nazionali e internazionali applicabili alla fornitura dei servizi TIC alle entità finanziarie.

4. Sulla base della valutazione di cui al paragrafo 2, e in coordinamento con la rete di sorveglianza comune di cui all'articolo 34, paragrafo 1, l'autorità di sorveglianza capofila adotta un piano di sorveglianza individuale chiaro, dettagliato e motivato che descrive gli obiettivi annuali in materia di sorveglianza e le principali azioni di sorveglianza previste per ciascun fornitore terzo critico di servizi TIC. Tale piano è comunicato annualmente al fornitore terzo critico di servizi TIC.

Prima dell'adozione del piano di sorveglianza, l'autorità di sorveglianza capofila comunica il progetto di piano di sorveglianza al fornitore terzo critico di servizi TIC.

Al ricevimento del progetto di piano di sorveglianza, il fornitore terzo critico di servizi TIC può presentare, entro 15 giorni di calendario, una dichiarazione motivata che dimostri l'impatto previsto sui clienti che sono entità che non rientrano nell'ambito di applicazione del presente regolamento e, se del caso, formuli soluzioni per attenuare i rischi.

5. Allorché i piani di sorveglianza annuali di cui al paragrafo 4 sono stati adottati e notificati ai fornitori terzi critici di servizi TIC, le autorità competenti possono adottare misure concernenti tali fornitori terzi critici di servizi TIC soltanto in accordo con l'autorità di sorveglianza capofila.

Articolo 34

Coordinamento operativo tra autorità di sorveglianza capofila

1. Per garantire un approccio coerente alle attività di sorveglianza e al fine di consentire strategie di sorveglianza generale coordinate e approcci operativi e metodologie di lavoro coerenti, le tre autorità di sorveglianza capofila nominate a norma dell'articolo 31, paragrafo 1, lettera b), istituiscono una rete di sorveglianza comune per coordinarsi tra loro nelle fasi preparatorie e coordinare lo svolgimento delle attività di sorveglianza sui rispettivi fornitori terzi critici di servizi TIC sottoposti a sorveglianza, nonché nello svolgimento di qualsiasi azione eventualmente necessaria a norma dell'articolo 42.

2. Ai fini del paragrafo 1, le autorità di sorveglianza capofila elaborano un protocollo comune di sorveglianza che specifica le procedure dettagliate da seguire per effettuare il coordinamento quotidiano e garantire scambi e reazioni rapidi. Il protocollo è riveduto periodicamente per tener conto delle esigenze operative, in particolare dell'evoluzione delle modalità pratiche di sorveglianza.

3. Le autorità di sorveglianza capofila possono, a seconda dei casi, chiedere alla BCE e all'ENISA di fornire consulenza tecnica, condividere esperienze pratiche o partecipare a specifiche riunioni di coordinamento della rete di sorveglianza comune.

Articolo 35

Poteri dell'autorità di sorveglianza capofila

1. Ai fini dello svolgimento dei compiti previsti dalla presente sezione, all'autorità di sorveglianza capofila sono conferiti i poteri indicati di seguito riguardo ai fornitori terzi critici di servizi TIC:

a) richiedere tutte le informazioni e la documentazione pertinenti ai sensi dell'articolo 37;

b) condurre indagini e ispezioni di carattere generale ai sensi degli articoli 38 e 39 rispettivamente;

c) richiedere, dopo il completamento delle attività di sorveglianza, relazioni in cui si specifichino le azioni adottate o i rimedi applicati da parte dei fornitori terzi critici di servizi TIC in relazione alle raccomandazioni di cui alla lettera d) del presente paragrafo;

d) formulare raccomandazioni concernenti i settori di cui all'articolo 33, paragrafo 3, in particolare per quanto riguarda gli elementi indicati di seguito:

   i) l'impiego di specifici processi o requisiti di sicurezza e qualità delle TIC, segnatamente per il rilascio di correzioni, aggiornamenti, cifratura e altre misure di sicurezza che l'autorità di sorveglianza capofila giudichi pertinenti per garantire la sicurezza delle TIC dei servizi forniti alle entità finanziarie;

   ii) l'uso di termini e condizioni, compresa la relativa attuazione tecnica, in base ai quali i fornitori terzi critici di servizi TIC prestano servizi TIC alle entità finanziarie, che l'autorità di sorveglianza capofila giudichi importanti per prevenire il prodursi di singoli punti di vulnerabilità (*points of failure*), l'amplificazione degli stessi, oppure per ridurre al minimo il possibile impatto sistemico in tutto il settore finanziario dell'Unione in caso di rischio di concentrazione delle TIC;

   iii) eventuali subappalti previsti, ove l'autorità di sorveglianza capofila ritenga che ulteriori subappalti, compresi gli accordi di subappalto che i fornitori terzi critici di servizi TIC intendano stipulare con fornitori terzi di servizi TIC o con subappaltatori di TIC stabiliti in un paese terzo, possano produrre rischi per la fornitura di servizi da parte dell'entità finanziaria o rischi per la stabilità finanziaria, sulla base dell'esame delle informazioni raccolte a norma degli articoli 37 e 38;

   iv) la rinuncia a stipulare un ulteriore accordo di subappalto qualora siano soddisfatte le condizioni cumulative seguenti:

      — il subappaltatore designato è un fornitore terzo di servizi TIC oppure un subappaltatore di TIC stabilito in un paese terzo;

      — il subappalto riguarda funzioni essenziali o importanti dell'entità finanziaria; nonché

— l'autorità di sorveglianza capofila ritiene che il ricorso a tale subappalto rappresenti un rischio grave e chiaro per la stabilità finanziaria dell'Unione o per le entità finanziarie, anche per quanto riguarda la capacità delle entità finanziarie di rispettare i requisiti in materia di sorveglianza.

Ai fini del punto iv) della presente lettera, i fornitori terzi di servizi TIC trasmettono all'autorità di sorveglianza capofila, utilizzando il modello di cui all'articolo 41, paragrafo 1, lettera b), le informazioni relative al subappalto.

2. Nell'esercizio dei poteri di cui al presente articolo, l'autorità di sorveglianza capofila:

a) assicura un coordinamento regolare all'interno della rete di sorveglianza comune e, in particolare, persegue approcci coerenti, se del caso, per quanto riguarda la sorveglianza dei fornitori terzi critici di servizi TIC;

b) tiene debitamente conto del quadro istituito dalla direttiva (UE) 2022/2555 e, se necessario, consulta le autorità competenti interessate designate o istituite in conformità di tale direttiva, al fine di evitare duplicazioni delle misure tecniche e organizzative che potrebbero applicarsi ai fornitori terzi critici di servizi TIC ai sensi di tale direttiva;

c) si adopera per ridurre al minimo, nella misura del possibile, il rischio di perturbazione dei servizi forniti da fornitori terzi critici di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento.

3. L'autorità di sorveglianza capofila consulta il forum di sorveglianza prima di esercitare i poteri di cui al paragrafo 1.

Prima di formulare raccomandazioni a norma del paragrafo 1, lettera d), l'autorità di sorveglianza capofila dà al fornitore terzo di servizi TIC la possibilità di fornire entro 30 giorni di calendario informazioni pertinenti che dimostrino l'impatto previsto sui clienti che sono entità che non rientrano nell'ambito di applicazione del presente regolamento e, se del caso, formulino soluzioni per attenuare i rischi.

4. L'autorità di sorveglianza capofila informa la rete di sorveglianza comune dell'esito dell'esercizio dei poteri di cui al paragrafo 1, lettere a) e b). L'autorità di sorveglianza capofila trasmette, senza indebito ritardo, le relazioni di cui al paragrafo 1, lettera c), alla rete di sorveglianza comune e alle autorità competenti delle entità finanziarie che utilizzano i servizi TIC di tale fornitore terzo critico di servizi TIC.

5. I fornitori terzi critici di servizi TIC cooperano in buona fede con l'autorità di sorveglianza capofila e la coadiuvano nell'adempimento dei suoi compiti.

6. In caso di inosservanza totale o parziale delle misure che devono essere adottate ai sensi dell'esercizio dei poteri di cui al paragrafo 1, lettere a), b) e c), e dopo la scadenza di un periodo di almeno 30 giorni di calendario dalla data in cui il fornitore terzo critico di servizi TIC ha ricevuto la notifica delle rispettive misure, l'autorità di sorveglianza capofila adotta una decisione che impone una penalità di mora al fine di costringere il fornitore terzo critico di servizi TIC a conformarsi a tali misure.

7. La penalità di mora, di cui al paragrafo 6, è imposta su base giornaliera fino al conseguimento della conformità e per un periodo non superiore a sei mesi dalla notifica della decisione che impone una penalità di mora al fornitore terzo critico di servizi TIC.

8. L'importo della penalità di mora, calcolato a partire dalla data indicata nella decisione che la impone, è fino all'1 % del fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo critico di servizi TIC nel precedente esercizio. Nel determinare l'importo della penalità, l'autorità di sorveglianza capofila tiene conto dei seguenti criteri per quanto riguarda l'inosservanza delle misure di cui al paragrafo 6:

a) la gravità e la durata dell'inosservanza;

b) se l'inosservanza sia stata commessa intenzionalmente o per negligenza;

c) il livello di cooperazione del fornitore terzo di servizi TIC con l'autorità di sorveglianza capofila.

Ai fini del primo comma, per garantire un approccio coerente, l'autorità di sorveglianza capofila avvia consultazioni nell'ambito della rete di sorveglianza comune.

9. Le penalità sono di natura amministrativa e sono esecutive. L'applicazione delle penalità è regolata dalle norme di procedura civile vigenti nello Stato membro sul cui territorio si svolgono le ispezioni e l'accesso. I giudici dello Stato membro interessato esercitano la giurisdizione sui reclami concernenti l'irregolarità dell'applicazione delle penalità. Gli importi delle penalità sono assegnati al bilancio generale dell'Unione europea.

10. L'autorità di sorveglianza capofila comunica al pubblico ogni penalità di mora inflitta, salvo il caso in cui tale comunicazione possa mettere gravemente a rischio i mercati finanziari o possa arrecare un danno sproporzionato alle parti coinvolte.

11. Prima di imporre una penalità di mora ai sensi del paragrafo 6, l'autorità di sorveglianza capofila concede ai rappresentanti del fornitore terzo critico di servizi TIC oggetto del procedimento l'opportunità di essere sentiti in merito alle risultanze, e fonda le proprie decisioni unicamente sulle risultanze in merito alle quali il fornitore terzo critico di servizi TIC oggetto del procedimento ha avuto la possibilità di esporre le proprie osservazioni.

Nel corso del procedimento sono pienamente garantiti i diritti della difesa delle persone interessate dal procedimento. Il fornitore terzo critico di servizi TIC oggetto del procedimento ha diritto di accesso al fascicolo, fermo restando il legittimo interesse di altre persone alla tutela dei propri segreti aziendali. Il diritto di accesso al fascicolo non si estende alle informazioni riservate o ai documenti preparatori interni dell'autorità di sorveglianza capofila.

Articolo 36

Esercizio dei poteri dell'autorità di sorveglianza capofila al di fuori dell'Unione

1. Qualora gli obiettivi di sorveglianza non possano essere conseguiti interagendo con l'impresa figlia istituita ai fini dell'articolo 31, paragrafo 12, o esercitando attività di sorveglianza in locali situati nell'Unione, l'autorità di sorveglianza capofila può esercitare i poteri, di cui alle disposizioni seguenti, in qualsiasi locale situato in un paese terzo che sia posseduto, o utilizzato in qualsiasi modo, ai fini della fornitura di servizi a entità finanziarie dell'Unione da parte di un fornitore terzo critico di servizi di TIC, riguardo alle relative operazioni commerciali, funzioni o servizi, compresi eventuali uffici amministrativi, commerciali o operativi, locali, terreni, edifici o altre proprietà:

a) articolo 35, paragrafo 1, lettera a); e

b) articolo 35, paragrafo 1, lettera b), conformemente all'articolo 38, paragrafo 2, lettere a), b) e d), e all'articolo 39, paragrafi 1 e 2, lettera a).

I poteri di cui al primo comma possono essere esercitati alle condizioni seguenti:

i) lo svolgimento di un'ispezione in un paese terzo è ritenuto necessario dall'autorità di sorveglianza capofila per consentirle di svolgere pienamente ed efficacemente i propri compiti ai sensi del presente regolamento;

ii) l'ispezione in un paese terzo è direttamente connessa alla fornitura di servizi TIC a entità finanziarie nell'Unione;

iii) il fornitore terzo critico di servizi TIC interessato acconsente allo svolgimento di un'ispezione in un paese terzo; nonché

iv) l'autorità pertinente del paese terzo interessato è stata ufficialmente informata dall'autorità di sorveglianza capofila e non ha sollevato obiezioni al riguardo.

2. Fatte salve le rispettive competenze delle istituzioni dell'Unione e degli Stati membri, ai fini del paragrafo 1, l'ABE, l'ESMA o l'EIOPA concludono accordi di cooperazione amministrativa con l'autorità pertinente del paese terzo al fine di consentire il regolare svolgimento delle ispezioni nel paese terzo interessato da parte dell'autorità di sorveglianza capofila e del gruppo designato per la sua missione in tale paese terzo. Tali accordi di cooperazione non creano obblighi giuridici per l'Unione e i suoi Stati membri, né impediscono agli Stati membri e alle loro autorità competenti di concludere accordi bilaterali o multilaterali con tali paesi terzi e le loro autorità pertinenti.

Tali accordi di cooperazione specificano almeno gli elementi seguenti:

a) le procedure per il coordinamento delle attività di sorveglianza svolte a norma del presente regolamento e qualsiasi analogo monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario esercitato dall'autorità pertinente del paese terzo interessato, comprese le modalità di trasmissione dell'accordo di quest'ultimo al fine di consentire all'autorità di sorveglianza capofila e al suo gruppo designato di svolgere le indagini generali e le ispezioni in loco di cui al paragrafo 1, primo comma, nel territorio sotto la sua giurisdizione;

b) il meccanismo per la trasmissione di tutte le informazioni pertinenti tra l'ABE, l'ESMA o l'EIOPA e l'autorità pertinente del paese terzo interessato, in particolare in relazione alle informazioni che possono essere richieste dall'autorità di sorveglianza capofila a norma dell'articolo 37;

c) i meccanismi per la tempestiva notifica, da parte dell'autorità pertinente del paese terzo interessato all'ABE, all'ESMA o all'EIOPA, dei casi in cui si ritiene che un fornitore terzo di servizi TIC stabilito in un paese terzo e designato come critico ai sensi dell'articolo 31, paragrafo 1, lettera a), abbia violato gli obblighi ai quali è tenuto a norma del diritto applicabile del paese terzo interessato quando fornisce servizi a enti finanziari in tale paese terzo, nonché i mezzi di ricorso e le penalità applicate;

d) la trasmissione periodica di aggiornamenti sugli sviluppi normativi o di vigilanza sul monitoraggio dei rischi informatici derivanti da terzi degli enti finanziari nel paese terzo interessato;

e) i dettagli per consentire, se necessario, la partecipazione di un rappresentante dell'autorità pertinente del paese terzo alle ispezioni condotte dall'autorità di sorveglianza capofila e dal gruppo designato.

3. Quando l'autorità di sorveglianza capofila non è in grado di svolgere le attività di sorveglianza, al di fuori dell'Unione, di cui ai paragrafi 1 e 2, l'autorità di sorveglianza capofila:

a) esercita i poteri di cui all'articolo 35 sulla base di tutti i fatti e di tutti i documenti di cui dispone;

b) documenta e spiega le eventuali conseguenze della sua incapacità di svolgere le attività di sorveglianza previste di cui al presente articolo.

Le potenziali conseguenze di cui alla lettera b) del presente comma sono prese in considerazione nelle raccomandazioni dell'autorità di sorveglianza capofila emesse a norma dell'articolo 35, paragrafo 1, lettera d).

Articolo 37

Richiesta di informazioni

1. L'autorità di sorveglianza capofila può, con semplice richiesta o mediante decisione, imporre ai fornitori terzi critici di servizi TIC di trasmettere tutte le informazioni necessarie all'autorità di sorveglianza capofila per adempiere i propri compiti ai sensi del presente regolamento, tra cui tutti i pertinenti documenti aziendali od operativi, contratti, documentazione strategica, relazioni di audit sulla sicurezza delle TIC, segnalazioni di incidenti informatici, nonché qualsiasi informazione relativa ai soggetti cui il fornitore terzo critico di servizi TIC ha esternalizzato attività o funzioni operative.

2. Quando invia una semplice richiesta di informazioni a norma del paragrafo 1, l'autorità di sorveglianza capofila:

a) fa riferimento al presente articolo quale base giuridica della richiesta;

b) dichiara la finalità della richiesta;

c) specifica le informazioni richieste;

d) stabilisce un termine entro il quale tali informazioni devono pervenirle;

e) informa il rappresentante critico del fornitore terzo di servizi TIC cui sono richieste le informazioni che non è tenuto a fornirle, ma in caso di risposta volontaria alla richiesta di informazioni, tali informazioni non devono essere inesatte né fuorvianti.

3. Quando impone mediante decisione la comunicazione di informazioni a norma del paragrafo 1, l'autorità di sorveglianza capofila:

a) fa riferimento al presente articolo quale base giuridica della richiesta;

b) dichiara la finalità della richiesta;

c) specifica le informazioni richieste;

d) stabilisce un termine entro il quale tali informazioni devono pervenirle;

e) indica le penalità di mora di cui all'articolo 35, paragrafo 6, laddove le informazioni fornite siano incomplete o quando tali informazioni non siano fornite entro il termine indicato alla lettera d) del presente paragrafo;

f) indica il diritto di presentare ricorso contro la decisione dinanzi alla commissione di ricorso dell'AEV e di adire la Corte di giustizia dell'Unione europea («Corte di giustizia») in conformità degli articoli 60 e 61 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

4. I rappresentanti dei fornitori terzi critici di servizi TIC forniscono le informazioni richieste. Gli avvocati debitamente incaricati possono fornire le informazioni richieste a nome dei loro clienti. I fornitori terzi critici di servizi TIC sono pienamente responsabili qualora le informazioni fornite siano incomplete, inesatte o fuorvianti.

5. L'autorità di sorveglianza capofila trasmette senza ritardo copia della decisione di fornire informazioni alle autorità competenti delle entità finanziarie che utilizzano i servizi dei fornitori terzi interessati di servizi TIC critici e alla rete di sorveglianza comune.

Articolo 38

Indagini generali

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila, coadiuvata dal gruppo di esaminatori congiunto di cui all'articolo 40, paragrafo 1, può, se necessario, svolgere le indagini sui fornitori terzi critici di servizi TIC.

2. L'autorità di sorveglianza capofila ha il potere di:

a) esaminare registri, dati, procedure e qualsiasi altro materiale pertinente per l'esecuzione dei compiti di sua competenza, su qualsiasi forma di supporto;

b) fare od ottenere copie certificate o estratti di tali registri, dati, procedure documentate e di ogni altro materiale;

c) convocare rappresentanti del fornitore terzo critico di servizi TIC e chiedere loro spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte;

d) interpellare persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine;

e) richiedere la documentazione relativa al traffico telefonico e al traffico dati.

3. I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila allo svolgimento dell'indagine di cui al paragrafo 1 esercitano i loro poteri dietro esibizione di un'autorizzazione scritta che specifichi l'oggetto e le finalità dell'indagine.

Tale autorizzazione indica anche la penalità di mora, di cui all'articolo 35, paragrafo 6, qualora i registri, i dati, le procedure documentate o qualsiasi altro materiale richiesto, oppure le risposte alle domande poste ai rappresentanti del fornitore terzo di servizi TIC, siano incompleti o non siano forniti affatto.

4. I rappresentanti dei fornitori terzi critici di servizi TIC sono tenuti a sottoporsi alle indagini sulla base di una decisione dell'autorità di sorveglianza capofila. La decisione specifica l'oggetto e le finalità dell'indagine nonché le penalità di mora di cui all'articolo 35, paragrafo 6, i mezzi di ricorso disponibili ai sensi dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010 e il diritto di ricorso dinanzi alla Corte di giustizia avverso la decisione.

5. In tempo utile prima dell'avvio dell'indagine, l'autorità di sorveglianza capofila informa le autorità competenti delle entità finanziarie che si avvalgono dei servizi TIC del fornitore terzo critico di servizi TIC in questione in merito all'indagine prevista e all'identità delle persone autorizzate.

L'autorità di sorveglianza capofila comunica alla rete di sorveglianza comune tutte le informazioni trasmesse a norma del primo comma.

Articolo 39

Ispezioni

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila può, coadiuvata dai gruppi di esaminatori congiunti di cui all'articolo 40, paragrafo 1, accedere a locali commerciali, immobili o proprietà dei fornitori terzi di servizi TIC, come sedi centrali, centri operativi, sedi secondarie, per condurvi tutte le necessarie ispezioni in loco; può inoltre effettuare ispezioni extra loco.

Ai fini dell'esercizio dei poteri di cui al primo comma, l'autorità di sorveglianza capofila consulta la rete di sorveglianza comune.

2. I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila a effettuare l'ispezione in loco hanno il potere di:

a) accedere ai suddetti locali commerciali, immobili o proprietà; e

b) sigillare i suddetti locali, libri o registri, per il periodo dell'ispezione e nella misura necessaria per effettuarla.

I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila esercitano i loro poteri dietro esibizione di un'autorizzazione scritta che specifichi l'oggetto e le finalità dell'ispezione, nonché le penalità di mora di cui all'articolo 35, paragrafo 6, qualora i rappresentanti dei fornitori terzi critici di servizi TIC interessati non si sottopongano all'ispezione.

3. In tempo utile prima dell'avvio dell'ispezione, l'autorità di sorveglianza capofila informa le autorità competenti delle entità finanziarie che si avvalgono di quel fornitore terzo di servizi TIC.

4. Le ispezioni si estendono all'intera gamma di sistemi, reti, dispositivi, informazioni e dati in materia di TIC utilizzati per la fornitura di servizi TIC alle entità finanziarie, o che vi contribuiscono.

5. Prima di qualsiasi ispezione in loco programmata, l'autorità di sorveglianza capofila concede un ragionevole preavviso ai fornitori terzi critici di servizi TIC, a meno che tale preavviso si riveli impossibile per una situazione di emergenza o di crisi, o qualora il preavviso rischi di provocare una situazione in cui l'ispezione o l'audit non sarebbero più efficaci.

6. Il fornitore terzo critico di servizi TIC si sottopone alle ispezioni in loco ordinate con decisione dell'autorità di sorveglianza capofila. La decisione specifica l'oggetto e le finalità dell'ispezione, fissa la data d'inizio dell'ispezione indica le penalità di mora di cui all'articolo 35, paragrafo 6, i mezzi di ricorso disponibili a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, nonché il diritto di presentare ricorso dinanzi alla Corte di giustizia avverso la decisione.

7. Qualora i funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila constatino che il fornitore terzo critico di servizi TIC si oppone all'ispezione ordinata ai sensi del presente articolo, l'autorità di sorveglianza capofila informa il fornitore terzo critico di servizi TIC delle conseguenze di tale opposizione, compresa la possibilità per le autorità competenti delle entità finanziarie interessate di imporre alle entità finanziarie di risolvere gli accordi contrattuali stipulati con il fornitore terzo critico di servizi TIC.

Articolo 40

Sorveglianza nel continuo

1. Nello svolgimento di attività di sorveglianza, in particolare indagini generali o ispezioni, l'autorità di sorveglianza capofila è coadiuvata da un gruppo di esaminatori congiunto istituito per ciascun fornitore terzo critico di servizi TIC.

2. Il gruppo di esaminatori congiunto di cui al paragrafo 1 è composto da membri del personale appartenenti:

a) alle AEV;

b) alle autorità competenti interessate che vigilano sulle entità finanziarie cui il fornitore terzo critico di servizi TIC presta servizi TIC;

c) all'autorità nazionale competente di cui all'articolo 32, paragrafo 4, lettera e), su base volontaria;

d) a un'autorità nazionale competente dello Stato membro in cui è stabilito il fornitore terzo critico di servizi TIC, su base volontaria.

I membri del gruppo di esaminatori congiunto possiedono competenze in materia di TIC e rischi operativi. Il gruppo di esaminatori congiunto è coordinato da un membro del personale dell'autorità di sorveglianza capofila designato a tale scopo («coordinatore dell'autorità di sorveglianza capofila»).

3. Entro tre mesi dal completamento dell'indagine o dell'ispezione, l'autorità di sorveglianza capofila, dopo essersi consultata con il forum di sorveglianza, adotta le raccomandazioni da inviare al fornitore terzo critico di servizi TIC in forza dei poteri che le sono stati conferiti ai sensi dell'articolo 35.

4. Le raccomandazioni di cui al paragrafo 3 sono comunicate immediatamente al fornitore terzo critico di servizi TIC e alle autorità competenti delle entità finanziarie cui il fornitore in questione presta i suoi servizi TIC.

Per l'espletamento delle attività di sorveglianza, l'autorità di sorveglianza capofila può tener conto di qualsiasi pertinente certificazione fornita da terzi e di relazioni di audit interni o esterni effettuati da terzi in materia di TIC messe a disposizione dal fornitore terzo critico di servizi TIC.

Articolo 41

Armonizzazione delle condizioni che consentono lo svolgimento delle attività di sorveglianza

1. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare:

a) le informazioni che il fornitore terzo di servizi TIC deve fornire nella domanda di designazione volontaria quale fornitore critico a norma dell'articolo 31, paragrafo 11;

b) il contenuto, la struttura e il formato delle informazioni da trasmettere, diffondere o segnalare da parte dei fornitori terzi di servizi TIC ai sensi dell'articolo 35, paragrafo 1, compreso il modello per fornire informazioni relative agli accordi di subappalto;

c) i criteri per determinare la composizione del gruppo di esaminatori congiunto, garantendo una partecipazione equilibrata dei membri del personale delle AEV e delle autorità competenti interessate, la loro nomina, i compiti e le modalità di lavoro.

d) i dettagli della valutazione, da parte delle autorità competenti, delle misure adottate dai fornitori terzi critici di servizi TIC sulla base delle raccomandazioni dell'autorità di sorveglianza capofila ai sensi dell'articolo 42, paragrafo 3.

2. Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 1, in conformità della procedura sancita agli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 42

Seguito dato dalle autorità competenti

1. Entro 60 giorni di calendario dalla ricezione delle raccomandazioni formulate dall'autorità di sorveglianza capofila ai sensi dell'articolo 35, paragrafo 1, lettera d), i fornitori terzi critici di servizi TIC comunicano all'autorità di sorveglianza capofila la loro intenzione di attenersi alle raccomandazioni o forniscono una spiegazione articolata del motivo per cui non lo faranno. L'autorità di sorveglianza capofila trasmette immediatamente le informazioni alle autorità competenti delle entità finanziarie interessate.

2. L'autorità di sorveglianza capofila rende pubblici i casi in cui un fornitore terzo critico di servizi TIC non dà notifica all'autorità di sorveglianza capofila conformemente al paragrafo 1 o se la spiegazione fornita dal fornitore terzo critico di servizi TIC non è ritenuta sufficiente. Le informazioni pubblicate rivelano l'identità del fornitore terzo critico di servizi TIC nonché informazioni sul tipo e la natura dell'inosservanza. Tali informazioni sono limitate a quanto è pertinente e proporzionato al fine di assicurare la sensibilizzazione del pubblico, salvo il caso in cui la pubblicazione possa arrecare un danno sproporzionato alle parti coinvolte o mettere gravemente a rischio il regolare funzionamento e l'integrità dei mercati finanziari o la stabilità dell'intero sistema finanziario dell'Unione o di parte di esso.

L'autorità di sorveglianza capofila informa il fornitore terzo di servizi TIC di tale divulgazione al pubblico.

3. Le autorità competenti informano le entità finanziarie interessate dei rischi individuati nelle raccomandazioni inviate ai fornitori terzi critici di servizi TIC conformemente all'articolo 35, paragrafo 1, lettera d).

Nella gestione dei rischi informatici derivanti da terzi, le entità finanziarie tengono conto dei rischi di cui al primo comma.

4. Qualora un'autorità competente ritenga che un'entità finanziaria non tenga conto dei rischi specifici individuati nelle raccomandazioni, o non li affronti in misura sufficiente, nell'ambito della sua gestione dei rischi informatici derivanti da terzi, essa notifica all'entità finanziaria la possibilità di adottare una decisione, entro 60 giorni di calendario dal ricevimento di tale notifica, a norma del paragrafo 6, in assenza di adeguati accordi contrattuali volti a far fronte a tali rischi.

5. Dopo aver ricevuto le relazioni di cui all'articolo 35, paragrafo 1, lettera c), e prima di adottare una decisione di cui al paragrafo 6 del presente articolo, le autorità competenti possono, su base volontaria, consultare le autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 responsabili della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come fornitore terzo critico di servizi TIC.

6. A norma dell'articolo 50, le autorità competenti possono adottare, come misura di ultima istanza, a seguito della notifica e, se del caso, della consultazione di cui ai paragrafi 4 e 5 del presente articolo, una decisione che impone alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore terzo critico di servizi TIC, fino a quando non siano stati affrontati i rischi identificati nelle raccomandazioni trasmesse ai fornitori terzi critici di servizi TIC. Laddove si renda necessario, le autorità competenti possono chiedere alle entità finanziarie di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con i fornitori terzi critici di servizi TIC.

7. Qualora un fornitore terzo critico di servizi TIC rifiuti di accogliere raccomandazioni basandosi su un approccio diverso da quello raccomandato dall'autorità di sorveglianza capofila e qualora tale approccio diverso possa avere un impatto negativo su un numero considerevole di entità finanziarie, o su una parte significativa del settore finanziario, e le singole segnalazioni emesse dalle autorità competenti non abbiano dato luogo ad approcci coerenti che attenuino il rischio potenziale per la stabilità finanziaria, l'autorità di sorveglianza capofila può, previa consultazione del forum di sorveglianza, emettere pareri non vincolanti e non pubblici alle autorità competenti, al fine di promuovere, se del caso, misure di follow-up coerenti e convergenti in materia di vigilanza.

8. Dopo aver ricevuto le relazioni di cui all'articolo 35, paragrafo 1, lettera c), le autorità competenti tengono conto, al momento di adottare le decisioni di cui al paragrafo 6 del presente articolo, del tipo e delle dimensioni del rischio che non è stato affrontato dal fornitore terzo critico di servizi TIC, nonché della gravità dell'inosservanza, in considerazione dei criteri seguenti:

a) la gravità e la durata dell'inosservanza;

b) se l'inosservanza abbia portato alla luce gravi carenze nelle procedure, nei sistemi di gestione, nella gestione dei rischi e nei controlli interni del fornitore terzo critico di servizi TIC;

c) se l'inosservanza abbia favorito o generato un reato finanziario o se tale reato sia in qualche misura attribuibile all'inosservanza;

d) se l'inosservanza sia stata commessa intenzionalmente o per negligenza;

e) se la sospensione o la risoluzione degli accordi contrattuali comporti un rischio per la continuità delle operazioni commerciali dell'entità finanziaria malgrado gli sforzi dell'entità finanziaria per evitare perturbazioni nella fornitura dei suoi servizi;

f) se del caso, il parere, richiesto su base volontaria conformemente al paragrafo 5 del presente articolo, delle autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555 responsabili della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come fornitore terzo critico di servizi TIC.

Le autorità competenti concedono alle entità finanziarie il periodo di tempo necessario per consentire loro di adeguare gli accordi contrattuali con i fornitori terzi critici di servizi TIC al fine di evitare effetti negativi sulla loro resilienza operativa digitale e di consentire loro di attuare le strategie di uscita e i piani di transizione di cui all'articolo 28.

9. La decisione di cui al paragrafo 6 del presente articolo è notificata ai membri del forum di sorveglianza di cui all'articolo 32, paragrafo 4, lettere a), b) e c), e alla rete di sorveglianza comune.

I fornitori terzi critici di servizi TIC interessati dalle decisioni di cui al paragrafo 6 cooperano pienamente con le entità finanziarie colpite, in particolare nel contesto del processo di sospensione o risoluzione dei loro accordi contrattuali.

10. Le autorità competenti informano l'autorità di sorveglianza capofila in merito alle misure e agli approcci adottati nell'ambito dei propri compiti di vigilanza in relazione alle entità finanziarie, nonché in merito agli accordi contrattuali conclusi da queste ultime qualora i fornitori terzi critici di servizi TIC abbiano disatteso, in tutto o in parte, le raccomandazioni loro rivolte dall'autorità di sorveglianza capofila.

11. L'autorità di sorveglianza capofila può, su richiesta, fornire ulteriori chiarimenti sulle raccomandazioni formulate per orientare le autorità competenti sulle misure di follow-up.

Articolo 43

Commissioni per le attività di sorveglianza

1. L'autorità di sorveglianza capofila addebita, conformemente all'atto delegato di cui al paragrafo 2 del presente articolo, ai fornitori terzi critici di servizi TIC commissioni che coprono completamente le spese necessarie sostenute dall'autorità di sorveglianza capofila in relazione allo svolgimento dei compiti di sorveglianza ai sensi del presente regolamento, compreso il rimborso dei costi eventualmente sostenuti in seguito al lavoro svolto dal gruppo di esaminatori congiunto di cui all'articolo 40, nonché i costi della consulenza fornita dagli esperti indipendenti di cui all'articolo 32, paragrafo 4, secondo comma, in relazione a questioni che rientrano nell'ambito delle attività di sorveglianza diretta.

L'importo della commissione addebitata al fornitore terzo critico di servizi TIC copre tutti i costi derivanti dall'esecuzione dei compiti di cui alla presente sezione ed è proporzionato al fatturato del fornitore.

2. Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 57, per integrare il presente regolamento determinando l'importo delle commissioni e le relative modalità di pagamento entro il 17 luglio 2024.

Articolo 44

Cooperazione internazionale

1. Fatto salvo l'articolo 36, ai sensi, rispettivamente, dell'articolo 33 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010, l'ABE, l'ESMA e l'EIOPA possono concludere accordi amministrativi con le autorità di vigilanza e di regolamentazione di paesi terzi per promuovere la cooperazione internazionale in materia di rischi informatici derivanti da terzi tra i diversi settori finanziari, in particolare definendo migliori prassi per il riesame delle pratiche e dei controlli per la gestione dei rischi informatici nonché per le misure di attenuazione e risposta agli incidenti.

2. Le AEV, tramite il comitato congiunto, presentano ogni cinque anni al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta riservata in cui sintetizzano le conclusioni delle discussioni pertinenti tenute con le autorità dei paesi terzi di cui al paragrafo 1, con particolare attenzione all'evoluzione dei rischi informatici derivanti da terzi e alle implicazioni per la stabilità finanziaria, l'integrità del mercato, la protezione degli investitori e il funzionamento del mercato interno.

CAPO VI

Meccanismi di condivisione delle informazioni

Articolo 45

Meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche

1. Le entità finanziarie possono scambiarsi reciprocamente informazioni e analisi delle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione, nella misura in cui tale condivisione di informazioni e dati:

a) mira a potenziare la resilienza operativa digitale delle entità finanziarie, in particolare aumentando la consapevolezza in merito alle minacce informatiche, contenendo o inibendo la capacità di diffusione delle minacce informatiche, sostenendo le capacità di difesa, le tecniche di individuazione delle minacce, le politiche di mitigazione o le fasi di risposta e ripristino;

b) si svolge entro comunità fidate di entità finanziarie;

c) si realizza mediante meccanismi di condivisione delle informazioni che tutelano la natura potenzialmente sensibile delle informazioni condivise e sono disciplinati da norme di condotta pienamente rispettose della riservatezza dell'attività economica, della protezione dei dati personali ai sensi del regolamento (UE) 2016/679 e delle linee guida sulla politica in materia di concorrenza.

2. Ai fini del paragrafo 1, lettera c), i meccanismi di condivisione delle informazioni definiscono le condizioni per la partecipazione e, se del caso, definiscono i dettagli concernenti il coinvolgimento delle autorità pubbliche e la veste in cui queste possono partecipare ai meccanismi di condivisione delle informazioni, il coinvolgimento dei fornitori terzi di servizi TIC, nonché gli elementi operativi tra cui l'utilizzo di piattaforme informatiche apposite.

3. Le entità finanziarie notificano alle autorità competenti la propria partecipazione ai meccanismi di condivisione delle informazioni di cui al paragrafo 1, al momento della convalida della propria adesione o, se del caso, della cessazione dell'adesione, quando quest'ultima abbia effetto.

CAPO VII

Autorità competenti

Articolo 46

Autorità competenti

Fatte salve le disposizioni sul quadro di sorveglianza per i fornitori terzi critici di servizi TIC di cui al capo V, sezione II, il rispetto del presente regolamento è assicurato dalle seguenti autorità competenti conformemente ai poteri conferiti dai rispettivi atti giuridici:

a) per gli enti creditizi e per gli enti esentati a norma della direttiva 2013/36/UE: l'autorità competente designata in conformità dell'articolo 4 di tale direttiva; e per gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013: la BCE conformemente ai poteri e ai compiti conferiti da tale regolamento;

b) per gli istituti di pagamento, compresi quelli esentati a norma della direttiva (UE) 2015/2366, gli istituti di moneta elettronica, compresi quelli esentati a norma della direttiva 2009/110/CE, e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366: l'autorità competente designata in conformità dell'articolo 22 della direttiva (UE) 2015/2366;

c) per le imprese di investimento: l'autorità competente designata in conformità dell'articolo 4 della direttiva (UE) 2019/2034 del Parlamento europeo e del Consiglio ([38]);

d) per i fornitori di servizi per le cripto-attività quali autorizzati ai sensi del regolamento sui mercati delle cripto-attività e gli emittenti di token collegati ad attività: l'autorità competente designata in conformità delle pertinenti disposizioni di tale regolamento;

e) per i depositari centrali di titoli: l'autorità competente designata in conformità dell'articolo 11 del regolamento (UE) n. 909/2014;

f) per le controparti centrali: l'autorità competente designata in conformità dell'articolo 22 del regolamento (UE) n. 648/2012;

g) per le sedi di negoziazione e i fornitori di servizi di comunicazione dati: l'autorità competente designata in conformità dell'articolo 67 della direttiva 2014/65/UE e l'autorità competente quale definita all'articolo 2, paragrafo 1, punto 18), del regolamento (UE) n. 600/2014;

h) per i repertori di dati sulle negoziazioni: l'autorità competente designata in conformità dell'articolo 22 del regolamento (UE) n. 648/2012;

i) per i gestori di fondi di investimento alternativi: l'autorità competente designata in conformità dell'articolo 44 della direttiva 2011/61/UE;

j) per le società di gestione: l'autorità competente designata in conformità dell'articolo 97 della direttiva 2009/65/CE;

k) per le imprese di assicurazione e di riassicurazione: l'autorità competente designata in conformità dell'articolo 30 della direttiva 2009/138/CE;

l) per gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi a titolo accessorio: l'autorità competente designata in conformità dell'articolo 12 della direttiva (UE) 2016/97;

m) per gli enti pensionistici aziendali o professionali: l'autorità competente designata a norma dell'articolo 47 della direttiva (UE) 2016/2341;

n) per le agenzie di rating del credito: l'autorità competente designata in conformità dell'articolo 21 del regolamento (CE) n. 1060/2009;

o) per gli amministratori di indici di riferimento critici: l'autorità competente designata in conformità degli articoli 40 e 41 del regolamento (UE) 2016/1011;

([38]) Direttiva (UE) 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).

p) per i fornitori di servizi di crowdfunding: l'autorità competente designata in conformità dell'articolo 29 del regolamento (UE) 2020/1503;

q) per i repertori di dati sulle cartolarizzazioni: l'autorità competente designata in conformità dell'articolo 10 e dell'articolo 14, paragrafo 1, del regolamento (UE) 2017/2402.

Articolo 47

Cooperazione con le strutture e le autorità istituite dalla direttiva (UE) 2022/2555

1. Per promuovere la cooperazione e consentire lo scambio di pratiche di vigilanza tra le autorità competenti designate a norma del presente regolamento e il gruppo di cooperazione istituito dall'articolo 14 della direttiva (UE) 2022/2555, le AEV e le autorità competenti possono partecipare alle attività del gruppo di cooperazione per le questioni che riguardano le loro attività di vigilanza in relazione alle entità finanziarie. Le AEV e le autorità competenti possono chiedere di essere invitate a partecipare alle attività del gruppo di cooperazione per questioni relative alle entità essenziali o importanti ai sensi della direttiva (UE) 2022/2555 che sono anch'esse state designate come fornitori terzi critici di servizi TIC a norma dell'articolo 31 del presente regolamento.

2. Le autorità competenti possono consultare, se del caso, i punti di contatto unici e i CSIRT designati o istituiti in conformità della direttiva (UE) 2022/2555, e scambiare informazioni con essi.

3. Se del caso, le autorità competenti possono richiedere qualsiasi consulenza e assistenza tecnica pertinenti alle autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555 e stabilire accordi di cooperazione per consentire l'istituzione di meccanismi di coordinamento efficaci e di risposta rapida.

4. Gli accordi di cui al paragrafo 3 del presente articolo possono, tra l'altro, specificare le procedure per il coordinamento delle attività di vigilanza e di sorveglianza, rispettivamente, in relazione a soggetti essenziali o importanti ai sensi della direttiva (UE) 2022/2555 che sono stati designati come fornitori terzi critici di servizi TIC a norma dell'articolo 31 del presente regolamento, anche per lo svolgimento, conformemente al diritto nazionale, di indagini e ispezioni in loco, nonché per i meccanismi per lo scambio di informazioni tra le autorità competenti ai sensi del presente regolamento e le autorità competenti designate o istituite a norma di tale direttiva, il che comprende l'accesso alle informazioni richieste da tali ultime autorità.

Articolo 48

Cooperazione tra autorità

1. Le autorità competenti cooperano strettamente tra loro e, se del caso, con l'autorità di sorveglianza capofila.

2. Le autorità competenti e l'autorità di sorveglianza capofila si scambiano tempestivamente tutte le informazioni pertinenti riguardanti i fornitori terzi critici di servizi TIC che sono necessarie per svolgere i rispettivi compiti ai sensi del presente regolamento, in particolare in relazione ai rischi individuati, agli approcci e alle misure adottate nell'ambito dei compiti di sorveglianza dell'autorità di sorveglianza capofila.

Articolo 49

Comunicazione, cooperazione e attività finanziarie intersettoriali

1. Le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, le autorità di risoluzione di cui all'articolo 3 della direttiva 2014/59/UE, la BCE, il Comitato di risoluzione unico per quanto riguarda le informazioni relative alle entità che rientrano nell'ambito di applicazione del regolamento (UE) n. 806/2014, il CERS e l'ENISA, se del caso, 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.

Le AEV 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'Unione nel caso di grave incidente transfrontaliero connesso alle TIC o relativa minaccia aventi un impatto sistemico sull'intero settore finanziario dell'Unione.

A seconda dei casi, tali esercitazioni possono anche servire come test delle dipendenze del settore finanziario da altri settori economici.

2. Le autorità competenti, le AEV e la BCE cooperano strettamente tra loro e si scambiano informazioni per svolgere i compiti di cui agli articoli da 47 a 54. Realizzano uno stretto coordinamento dell'attività di vigilanza per rilevare e correggere le violazioni del presente regolamento, sviluppare e promuovere migliori prassi, agevolare la collaborazione, promuovere la coerenza dell'interpretazione e formulare valutazioni transgiurisdizionali in caso di disaccordo.

Articolo 50

Sanzioni amministrative e misure di riparazione

1. Alle autorità competenti sono conferiti tutti i poteri di vigilanza, di indagine e sanzionatori necessari per adempiere i propri compiti ai sensi del presente regolamento.

2. I poteri di cui al paragrafo 1 includono almeno i poteri seguenti:

a) l'avere accesso a qualsiasi documento o dato, detenuto in qualsiasi forma, che l'autorità competente consideri pertinente per lo svolgimento dei propri compiti e la possibilità di riceverne o farne una copia;

b) lo svolgere ispezioni o indagini in loco comprendenti tra l'altro:

   i) la convocazione di rappresentanti delle entità finanziarie per ottenere spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte;

   ii) l'audizione di persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine;

c) il richiedere l'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del presente regolamento.

3. Fatto salvo il diritto degli Stati membri di imporre sanzioni penali in conformità dell'articolo 52, gli Stati membri stabiliscono norme che prevedano adeguate sanzioni amministrative e misure di riparazione per le violazioni del presente regolamento e ne garantiscono l'effettiva applicazione.

Tali sanzioni e misure sono efficaci, proporzionate e dissuasive.

4. Gli Stati membri conferiscono alle autorità competenti il potere di applicare almeno le sanzioni amministrative o misure di riparazione seguenti per le violazioni del presente regolamento:

a) emanare un ordine che imponga alla persona fisica o giuridica di porre termine al comportamento in violazione del presente regolamento e di astenersi dal ripeterlo;

b) richiedere la cessazione temporanea o permanente di qualsiasi pratica o comportamento che le autorità competenti considerino contrari alle disposizioni del presente regolamento e prevenirne la reiterazione;

c) adottare qualsiasi tipo di misura, anche di natura pecuniaria, per assicurare che le entità finanziarie continuino a rispettare i requisiti di legge;

d) chiedere, nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti di traffico dati detenute dagli operatori di telecomunicazioni, qualora vi sia il ragionevole sospetto di violazioni del presente regolamento e qualora si ritenga che le registrazioni possano essere pertinenti ai fini delle rispettive indagini; nonché

e) pubblicare comunicazioni pubbliche, comprese dichiarazioni pubbliche, indicanti l'identità della persona fisica o giuridica e la natura della violazione.

5. Qualora il paragrafo 2, lettera c), e il paragrafo 4 si applichino a persone giuridiche, gli Stati membri conferiscono alle autorità competenti il potere di imporre sanzioni amministrative e misure di riparazione, alle condizioni previste dal diritto nazionale, nei confronti di membri dell'organo di gestione e di altre persone che, ai sensi del diritto nazionale, siano responsabili della violazione.

6. Gli Stati membri garantiscono che qualsiasi decisione di imporre sanzioni amministrative o misure di riparazione adottata ai sensi del paragrafo 2, lettera c), sia adeguatamente motivata e preveda il diritto di ricorso.

Articolo 51

Esercizio del potere di imporre sanzioni amministrative e misure di riparazione

1. Le autorità competenti esercitano il potere di imporre sanzioni amministrative e misure di riparazione di cui all'articolo 50 in conformità del proprio quadro giuridico nazionale, a seconda dei casi:

a) direttamente;

b) in collaborazione con altre autorità;

c) sotto la propria responsabilità mediante delega ad altre autorità; oppure

d) rivolgendosi alle competenti autorità giudiziarie.

2. Per stabilire il tipo e il livello della sanzione amministrativa o della misura di riparazione da imporre a norma dell'articolo 50, le autorità competenti tengono conto della misura in cui la violazione è intenzionale o è dovuta a negligenza e di tutte le altre circostanze pertinenti, tra cui, secondo il caso:

a) la rilevanza, la gravità e la durata della violazione;

b) il grado di responsabilità della persona fisica o giuridica responsabile della violazione;

c) la solidità finanziaria della persona fisica o giuridica responsabile;

d) l'importanza degli utili realizzati o delle perdite evitate da parte della persona fisica o giuridica responsabile, nella misura in cui possano essere determinati;

e) le perdite subite da terzi a causa della violazione, nella misura in cui possano essere determinate;

f) il livello di cooperazione che la persona fisica o giuridica responsabile ha dimostrato nei confronti dell'autorità competente, ferma restando la necessità di garantire la restituzione degli utili realizzati o delle perdite evitate da tale persona fisica o giuridica;

g) le precedenti violazioni commesse dalla persona fisica o giuridica responsabile.

Articolo 52

Sanzioni penali

1. Gli Stati membri possono decidere di non emanare norme relative a sanzioni amministrative o misure di riparazione per violazioni che, ai sensi del rispettivo diritto nazionale, siano passibili di sanzioni penali.

2. Qualora abbiano deciso di imporre sanzioni penali per violazioni del presente regolamento, gli Stati membri provvedono affinché siano messe in atto misure adeguate per far sì che le autorità competenti dispongano di tutti i poteri necessari per stabilire contatti con le autorità giudiziarie, le autorità inquirenti o le autorità di giustizia penale della loro giurisdizione, al fine di ricevere informazioni specifiche sulle indagini o i procedimenti penali avviati per violazioni del presente regolamento, e di trasmetterle alle altre autorità competenti, nonché all'ABE, all'ESMA o all'EIOPA in modo tale che possano adempiere l'obbligo di cooperazione ai fini del presente regolamento.

Articolo 53

Obblighi di notifica

Gli Stati membri notificano alla Commissione, all'ESMA, all'ABE e all'EIOPA le disposizioni legislative, regolamentari e amministrative adottate in attuazione del presente capo, incluse le eventuali norme di diritto penale pertinenti, entro il 17 gennaio 2025. Gli Stati membri notificano senza indebito ritardo alla Commissione, all'ESMA, all'ABE e all'EIOPA tutte le successive modifiche.

Articolo 54

Pubblicazione delle sanzioni amministrative

1. Le autorità competenti pubblicano senza indebito ritardo sul proprio sito web ufficiale qualsiasi decisione di imporre sanzioni amministrative contro la quale non vi sia diritto di ricorso, dopo la notifica al destinatario.

2. La pubblicazione di cui al paragrafo 1 comprende informazioni sul tipo e la natura della violazione, l'identità delle persone responsabili e le sanzioni imposte.

3. Qualora, in seguito a una valutazione caso per caso, ritenga che la pubblicazione dell'identità, nel caso di persone giuridiche, o dell'identità e dei dati personali, nel caso di persone fisiche, sarebbe sproporzionata, ivi compresi rischi inerenti alla protezione dei dati personali, metterebbe a repentaglio la stabilità dei mercati finanziari o lo svolgimento di un'indagine penale in corso, oppure provocherebbe, nella misura in cui possano essere determinati, danni sproporzionati alla persona coinvolta, l'autorità competente adotta una delle soluzioni seguenti in merito alla decisione di imporre una sanzione amministrativa:

a) rinvia la pubblicazione fino al momento in cui cesseranno di esistere tutti i motivi che giustificano la non pubblicazione;

b) pubblica la sanzione in forma anonima in maniera conforme al diritto nazionale; oppure

c) si astiene dalla pubblicazione, qualora le opzioni di cui alle lettere a) e b) siano ritenute insufficienti per scongiurare ogni pericolo per la stabilità dei mercati finanziari, oppure quando tale pubblicazione non sarebbe proporzionata alla mitezza della sanzione imposta.

4. Qualora si decida di pubblicare una sanzione amministrativa in forma anonima, ai sensi del paragrafo 3, lettera b), la pubblicazione dei dati pertinenti può essere rinviata.

5. Qualora l'autorità competente pubblichi una decisione che impone una sanzione amministrativa che è oggetto di ricorso dinanzi alle pertinenti autorità giudiziarie, le autorità competenti aggiungono immediatamente sul proprio sito web ufficiale tale informazione e, nelle fasi successive, eventuali informazioni correlate all'esito del ricorso. È pubblicata anche ogni decisione giudiziaria che annulli una decisione di imporre una sanzione amministrativa.

6. Le autorità competenti provvedono affinché le informazioni pubblicate ai sensi dei paragrafi da 1 a 4 restino sul loro sito web ufficiale unicamente per il periodo necessario ai fini dell'applicazione del presente articolo. Tale periodo non è superiore ai cinque anni dalla sua pubblicazione.

Articolo 55

Segreto professionale

1. Le informazioni riservate ricevute, scambiate o trasmesse a norma del presente regolamento sono soggette alle condizioni in materia di segreto professionale di cui al paragrafo 2.

2. L'obbligo del segreto professionale si applica a tutte le persone che prestano o hanno prestato la loro attività per le autorità competenti ai sensi del presente regolamento o per qualsiasi autorità, impresa che opera sul mercato o persona fisica o giuridica cui tali autorità competenti hanno delegato i propri poteri, compresi i revisori e gli esperti incaricati da dette autorità.

3. Le informazioni coperte dal segreto professionale, ivi compreso lo scambio di informazioni tra le autorità competenti ai sensi del presente regolamento e le autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555, non sono divulgate ad alcuna altra persona o autorità se non in forza di disposizioni del diritto dell'Unione o del diritto nazionale;

4. Tutte le informazioni scambiate tra le autorità competenti in applicazione del presente regolamento relativamente ad aspetti commerciali od operativi e ad altre questioni di natura economica o personale sono considerate riservate e sono soggette all'obbligo del segreto professionale, salvo quando l'autorità competente dichiara al momento della loro comunicazione che è consentita la divulgazione di tali informazioni o che la stessa è necessaria a fini di procedimenti giudiziari.

Articolo 56

Protezione dei dati

1. Le AEV e le autorità competenti sono autorizzate a trattare i dati personali solo se necessario ai fini dell'adempimento dei rispettivi obblighi e doveri ai sensi del presente regolamento, in particolare per quanto riguarda le indagini, le ispezioni, la richiesta di informazioni, la comunicazione, la pubblicazione, le valutazioni, la verifica e la stesura dei piani di sorveglianza. I dati personali sono trattati a norma del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, a seconda dei casi.

2. Salvo nel caso in cui sia altrimenti disposto in altri atti settoriali, i dati personali di cui al paragrafo 1 sono conservati fino all'espletamento degli obblighi di vigilanza applicabili e, in ogni caso, per un periodo massimo di 15 anni, salvo in caso di procedimenti giudiziari in corso che richiedono un'ulteriore conservazione di tali dati.

CAPO VIII

Atti delegati

Articolo 57

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 31, paragrafo 6, e all'articolo 43, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 17 gennaio 2024. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 31, paragrafo 6, e all'articolo 43, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 31, paragrafo 6, e dell'articolo 43, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

CAPO IX

Disposizioni transitorie e finali

Sezione I

Articolo 58

Clausola di riesame

1. Entro il 17 gennaio 2028, la Commissione, dopo aver consultato le AEV e il CERS, a seconda dei casi, effettua un riesame e presenta al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa. Il riesame comprende almeno:

a) i criteri per la designazione dei fornitori terzi critici di servizi TIC, di cui all'articolo 31, paragrafo 2;

b) il carattere volontario della notifica di minacce informatiche significative di cui all'articolo 19;

c) il regime di cui all'articolo 31, paragrafo 12, e i poteri dell'autorità di sorveglianza capofila di cui all'articolo 35, paragrafo 1, lettera d), punto iv), primo trattino, al fine di valutare l'efficacia di tali disposizioni per quanto riguarda la garanzia di una sorveglianza efficace dei fornitori terzi critici di servizi TIC stabiliti in un paese terzo e la necessità di istituire un'impresa figlia nell'Unione.

   Ai fini del primo comma della presente lettera, il riesame comprende un'analisi del regime di cui all'articolo 31, paragrafo 12, comprese le condizioni di accesso delle entità finanziarie dell'Unione ai servizi di paesi terzi e la disponibilità di tali servizi sul mercato dell'Unione, e tiene conto degli ulteriori sviluppi nei mercati dei servizi disciplinati dal presente regolamento, dell'esperienza pratica delle entità finanziarie e delle autorità di vigilanza finanziaria per quanto riguarda l'applicazione e, rispettivamente, la vigilanza di tale regime e di eventuali sviluppi pertinenti in materia di regolamentazione e vigilanza a livello internazionale;

d) se sia opportuno includere nell'ambito di applicazione del presente regolamento le entità finanziarie di cui all'articolo 2, paragrafo 3, lettera e), che utilizzano sistemi di vendita automatizzata, alla luce dei futuri sviluppi del mercato sull'uso di tali sistemi;

e) il funzionamento e l'efficacia della rete di sorveglianza comune in termini di sostegno alla coerenza della sorveglianza e all'efficienza dello scambio di informazioni nell'ambito del quadro di sorveglianza.

2. Nel contesto del riesame della direttiva (UE) 2015/2366, la Commissione valuta la necessità di una maggiore ciberresilienza dei sistemi di pagamento e delle attività di trattamento dei pagamenti e se sia opportuno ampliare l'ambito di applicazione del presente regolamento agli operatori dei sistemi di pagamento e alle entità coinvolte nelle attività di trattamento dei pagamenti. Alla luce di tale valutazione, la Commissione presenta, nell'ambito del riesame della direttiva (UE) 2015/2366, una relazione al Parlamento europeo e al Consiglio e entro il 17 luglio 2023.

Sulla base di tale relazione di riesame e previa consultazione delle AEV, della BCE e del CERS, la Commissione può presentare, se del caso e nell'ambito della proposta legislativa che può adottare a norma dell'articolo 108, secondo comma, della direttiva (UE) 2015/2366, una proposta volta a garantire che tutti gli operatori dei sistemi di pagamento e le entità coinvolte nelle attività di trattamento dei pagamenti siano soggetti a un'adeguata sorveglianza, tenendo conto nel contempo dell'esistente sorveglianza da parte delle banche centrali.

3. Entro il 17 gennaio 2026, la Commissione, dopo aver consultato le AEV e il comitato degli organismi europei di controllo delle attività di revisione contabile, effettua un riesame e presenta al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa sull'opportunità di rafforzare i requisiti per i revisori legali e le imprese di revisione contabile per quanto riguarda la resilienza operativa digitale, mediante l'inclusione dei revisori legali e delle imprese di revisione contabile nell'ambito di applicazione del presente regolamento o mediante modifiche della direttiva 2006/43/CE del Parlamento europeo e del Consiglio ([39]).

Sezione II

Modifiche

Articolo 59

Modifiche del regolamento (CE) n. 1060/2009

Il regolamento (CE) n. 1060/2009 è così modificato:

1) nell'allegato I, sezione A, punto 4, il primo comma è sostituito dal seguente:

«Un'agenzia di rating del credito dispone di procedure amministrative e contabili solide, di meccanismi di controllo interno, di procedure efficaci per la valutazione del rischio e di meccanismi efficaci di controllo e protezione per la gestione dei sistemi di TIC in conformità del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

2) nell'allegato III, il punto 12) è sostituito dal seguente:

«12) L'agenzia di rating del credito viola l'articolo 6, paragrafo 2, in combinato disposto con l'allegato I, sezione A, punto 4, quando non dispone di procedure amministrative o contabili solide, di meccanismi di controllo interno, di procedure efficaci per la valutazione del rischio o di meccanismi efficaci di controllo e protezione per la gestione dei sistemi di TIC in conformità del regolamento (UE) 2022/2554, o non instaurando, né mantenendo le procedure di adozione di decisione o le strutture organizzative richieste dal predetto punto.».

Articolo 60

Modifiche del regolamento (UE) n. 648/2012

Il regolamento (UE) n. 648/2012 è così modificato:

1) l'articolo 26 è così modificato:

a) il paragrafo 3 è sostituito dal seguente:

«3. Le CCP mantengono e gestiscono una struttura organizzativa che assicuri la continuità e il regolare funzionamento della prestazione dei servizi e dell'esercizio delle attività. Esse utilizzano sistemi, risorse e procedure adeguati e proporzionati, tra cui sistemi di TIC gestiti in conformità del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

([39]) 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).

b) il paragrafo 6 è soppresso;

2) l'articolo 34 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Le CCP adottano, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendenti una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC predisposti e attuati in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi della CCP.»;

b) al paragrafo 3, il primo comma è sostituito dal seguente:

«3. Al fine di garantire l'applicazione coerente del presente articolo, l'ESMA, previa consultazione dei membri del SEBC, elabora progetti di norme tecniche di regolamentazione per specificare il contenuto minimo e i requisiti della politica di continuità operativa e del piano di ripristino in caso di disastro, con l'esclusione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC.»;

3) all'articolo 56, paragrafo 3, il primo comma è sostituito dal seguente:

«3. Per assicurare l'applicazione uniforme del presente articolo, l'ESMA elabora progetti di norme tecniche di regolamentazione che specifichino, tranne che per i requisiti in materia di gestione dei rischi informatici, i dettagli della domanda di registrazione di cui al paragrafo 1.»;

4) all'articolo 79, i paragrafi 1 e 2 sono sostituiti dai seguenti:

«1. I repertori di dati sulle negoziazioni individuano le fonti di rischio operativo e le riducono anche sviluppando sistemi, controlli e procedure adeguati, tra cui sistemi di TIC gestiti ai sensi del regolamento (UE) 2022/2554.

2. I repertori di dati sulle negoziazioni stabiliscono, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendenti una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle loro funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti.»;

5) all'articolo 80, il paragrafo 1 è soppresso;

6) nell'allegato I, la sezione II è così modificata:

a) le lettere a) e b) sono sostituite dalle seguenti:

«a) un repertorio di dati sulle negoziazioni viola l'articolo 79, paragrafo 1, allorché non individua le fonti di rischio operativo o non limita al massimo tali rischi sviluppando sistemi, controlli e procedure adeguati, tra cui sistemi di TIC gestiti ai sensi del regolamento (UE) 2022/2554;

b) un repertorio di dati sulle negoziazioni viola l'articolo 79, paragrafo 2, allorché non stabilisce, non attua o non mantiene una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle proprie funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti;»;

b) la lettera c) è soppressa;

7) l'allegato III è così modificato:

a) La sezione II è così modificata:

i) la lettera c) è sostituita dalla seguente:

«c) una CCP di classe 2 viola l'articolo 26, paragrafo 3, allorché non mantiene o non gestisce una struttura organizzativa che assicuri la continuità e il regolare funzionamento della prestazione dei propri servizi e dell'esercizio delle attività, o allorché non utilizza sistemi, risorse o procedure adeguati e proporzionati, tra cui sistemi di TIC gestiti conformemente al regolamento (UE) 2022/2554»;

ii) la lettera f) è soppressa;

b) nella sezione III, la lettera a) è sostituita dalla seguente:

«a) una CCP di classe 2 viola l'articolo 34, paragrafo 1, allorché non stabilisce, non attua o non mantiene una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle proprie funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti dalla CCP; tale piano prevede almeno la ripresa di tutte le operazioni in corso al momento della perturbazione in modo da permettere alla CCP di continuare a funzionare con certezza e di completare il regolamento alla data prevista;».

Articolo 61

Modifiche del regolamento (UE) n. 909/2014

L'articolo 45 del regolamento (UE) n. 909/2014 è così modificato:

1) il paragrafo 1 è sostituito dal seguente:

«1. I CSD individuano le fonti di rischio operativo, interne ed esterne, e ne riducono al minimo l'impatto avvalendosi di strumenti, processi e politiche in materia di TIC adeguati, istituiti e gestiti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché mediante qualsiasi altro tipo adeguato di strumenti, controlli e procedure per altri tipi di rischi operativi, anche per tutti i sistemi di regolamento titoli da essi operati.

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

2) il paragrafo 2 è soppresso;

3) i paragrafi 3 e 4 sono sostituiti dai seguenti:

«3. Per i servizi che forniscono nonché per ciascun sistema di regolamento titoli da essi operato, i CSD stabiliscono, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendente una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti ai sensi del regolamento (UE) 2022/2554, allo scopo di preservare i servizi, assicurare la ripresa tempestiva delle attività e l'adempimento degli obblighi del CSD in caso di eventi che comportino un rischio significativo di perturbare le attività.

4. Il piano di cui al paragrafo 3 prevede il ripristino di tutte le operazioni e posizioni dei partecipanti al momento della perturbazione, in modo da permettere ai partecipanti al CSD di continuare ad operare con certezza e di completare il regolamento alla data prevista, anche assicurando che i sistemi informatici critici possano riprendere a funzionare dal momento della perturbazione, come previsto dall'articolo 12, paragrafi 5 e 7, del regolamento (UE) 2022/2554.»;

4) il paragrafo 6 è sostituito dal seguente:

«6. I CSD individuano, controllano e gestiscono i rischi ai quali i principali partecipanti ai sistemi di regolamento titoli da essi operati nonché i fornitori di servizi e utenze, e altri CSD o altre infrastrutture di mercato possono esporre le loro attività. Su richiesta, forniscono alle autorità competenti e alle autorità rilevanti informazioni su ogni rischio siffatto individuato. Informano inoltre senza ritardo l'autorità competente e le autorità rilevanti in merito a eventuali incidenti operativi causati da tali rischi, tranne che in relazione ai rischi informatici.»;

5) al paragrafo 7, il primo comma è sostituito dal seguente:

«7. L'ESMA, in stretta cooperazione con i membri del SEBC, elabora progetti di norme tecniche di regolamentazione per specificare i rischi operativi di cui ai paragrafi 1 e 6, tranne che in relazione ai rischi informatici, i metodi per testare, gestire o ridurre al minimo tali rischi, ivi compresi le politiche di continuità operativa e i piani di ripristino in caso di disastro di cui ai paragrafi 3 e 4, nonché i metodi di valutazione degli stessi.».

Articolo 62

Modifiche del regolamento (UE) n. 600/2014

Il regolamento (UE) n. 600/2014 è così modificato:

1) l'articolo 27 *octies* è così modificato:

a) il paragrafo 4 è sostituito dal seguente:

«4. Gli APA rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

_____

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

b) al paragrafo 8, la lettera c) è sostituita dalla seguente:

«c) i requisiti organizzativi concreti di cui ai paragrafi 3 e 5.»;

2) l'articolo 27 *nonies* è così modificato:

a) il paragrafo 5 è sostituito dal seguente:

«5. I CTP rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554.»;

b) al paragrafo 8, la lettera e) è sostituita dalla seguente:

«e) i requisiti organizzativi concreti di cui al paragrafo 4.»;

3) l'articolo 27 *decies* è così modificato:

a) il paragrafo 3 è sostituito dal seguente:

«3. Gli ARM rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554.»;

b) al paragrafo 5, la lettera b) è sostituita dalla seguente:

«b) i requisiti organizzativi concreti di cui ai paragrafi 2 e 4.».

Articolo 63

Modifiche del regolamento (UE) 2016/1011

All'articolo 6 del regolamento (UE) 2016/1011 è aggiunto il paragrafo seguente:

«6. Per gli indici di riferimento critici, un amministratore dispone di procedure amministrative e contabili solide, di meccanismi di controllo interno, di procedure efficaci per la valutazione del rischio e di meccanismi efficaci di controllo e protezione per la gestione dei sistemi di TIC in conformità del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

_____

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

Articolo 64

Entrata in vigore e applicazione

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

Esso si applica a decorrere dal 17 gennaio 2025.

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

Fatto a Strasburgo, il 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK

DIRETTIVE

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)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea ([1]),

visto il parere del Comitato economico e sociale europeo ([2]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([4]) mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, a mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società.

(2) Dall'entrata in vigore della direttiva (UE) 2016/1148 sono stati compiuti progressi significativi nell'aumentare il livello dell'Unione in materia di ciberresilienza. La revisione di tale direttiva ha mostrato quanto quest'ultima sia servita da catalizzatore per l'approccio istituzionale e normativo alla cibersicurezza nell'Unione, aprendo la strada a un significativo cambiamento della mentalità. Tale direttiva ha garantito il completamento dei quadri nazionali sulla sicurezza dei sistemi informatici e di rete definendo le strategie nazionali sulla sicurezza dei sistemi informatici e di rete e stabilendo capacità nazionali e attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. La direttiva (UE) 2016/1148 ha inoltre contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione e della rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente. Nonostante tali risultati, la revisione della direttiva (UE) 2016/1148 ha rivelato carenze intrinseche che le impediscono di affrontare efficacemente le sfide attuali ed emergenti in materia di cibersicurezza.

(3) I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete. Tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato

([1]) GU C 233 del 16.6.2022, pag. 22.
([2]) GU C 286 del 16.7.2021, pag. 170.
([3]) Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.
([4]) 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).

interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno. Inoltre, la cibersicurezza è un fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione.

(4) La base giuridica della direttiva (UE) 2016/1148 era l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Gli obblighi di cibersicurezza imposti ai soggetti che forniscono servizi o svolgono attività economicamente rilevanti variano notevolmente da uno Stato membro all'altro in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza. Tali disparità comportano costi aggiuntivi e creano difficoltà per le entità che offrono beni o servizi transfrontalieri. Gli obblighi imposti da uno Stato membro che sono diversi o addirittura in conflitto con quelli imposti da un altro Stato membro possono incidere in modo sostanziale su tali attività transfrontaliere. Inoltre, è probabile che una progettazione o attuazione inadeguata degli obblighi in materia di cibersicurezza in uno Stato membro abbia ripercussioni sul livello di cibersicurezza di altri Stati membri, in particolare in considerazione dell'intensità degli scambi transfrontalieri. Il riesame della direttiva (UE) 2016/1148 ha evidenziato notevoli divergenze nella sua attuazione da parte degli Stati membri, anche per quanto riguarda il suo ambito di applicazione, la cui delimitazione è stata lasciata in larga misura alla discrezione degli Stati membri. La direttiva (UE) 2016/1148 ha inoltre conferito agli Stati membri un ampio potere discrezionale per quanto riguarda l'attuazione degli obblighi in materia di sicurezza e segnalazione degli incidenti ivi stabiliti. Tali obblighi sono stati pertanto attuati in modi significativamente diversi a livello nazionale. Analoghe divergenze sussistono nell'attuazione delle disposizioni della direttiva (UE) 2016/1148 in materia di vigilanza e esecuzione.

(5) Tutte tali divergenze comportano una frammentazione del mercato interno e possono avere un effetto pregiudizievole sul suo funzionamento, con ripercussioni in particolare sulla fornitura transfrontaliera di servizi e sul livello di ciberresilienza dovute all'applicazione di misure diverse. Dette divergenze possono portare infine a una maggiore vulnerabilità di taluni Stati membri di fronte alle minacce informatiche, con potenziali ricadute sull'intera Unione. La presente direttiva mira a eliminare tali ampie divergenze tra gli Stati membri, in particolare stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili in ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e prevedendo mezzi di ricorso e misure di esecuzione effettivi che siano funzionali all'efficace applicazione di tali obblighi. La direttiva (UE) 2016/1148 dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(6) Con l'abrogazione della direttiva (UE) 2016/1148, l'ambito di applicazione per settore dovrebbe essere esteso a una parte più ampia dell'economia per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche nel mercato interno. In particolare, la presente direttiva mira a superare le carenze della differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, che si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.

(7) Ai sensi della direttiva (UE) 2016/1148, gli Stati membri erano responsabili di identificare i soggetti che soddisfacevano i criteri per essere considerati operatori di servizi essenziali. Al fine di eliminare le ampie divergenze tra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione per tutti i soggetti pertinenti, è opportuno stabilire un criterio uniforme che determini quali soggetti rientrano nell'ambito di applicazione della presente direttiva. Tale criterio dovrebbe consistere nell'applicazione di una regola della soglia di dimensione, in base alla quale si considerano medie imprese ai sensi dell'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE della Commissione ([5]), o superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che operano

([5]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

nei settori e forniscono le tipologie di servizi o svolgono le attività contemplati dalla presente direttiva. Gli Stati membri dovrebbero inoltre prevedere che determinate piccole imprese e microimprese, quali definite all'articolo 2, paragrafi 2 e 3, di tale allegato, che soddisfano criteri specifici che indicano un ruolo chiave per la società, l'economia o per particolari settori o tipi di servizi rientrino nell'ambito di applicazione della presente direttiva.

(8) L'esclusione degli enti della pubblica amministrazione dall'ambito di applicazione della presente direttiva dovrebbe applicarsi ai soggetti che operano principalmente nei settori della sicurezza nazionale, della sicurezza pubblica, della difesa o svolgono attività di contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati. Tuttavia, gli enti della pubblica amministrazione le cui attività sono solo marginalmente connesse a tali settori non dovrebbero essere esclusi dall'ambito di applicazione della presente direttiva. Ai fini della presente direttiva, non si considera che i soggetti con competenze normative operino nel settore dell'attività di contrasto e pertanto essi non sono esclusi su tale base dall'ambito di applicazione della presente direttiva. Gli enti della pubblica amministrazione istituiti congiuntamente con un paese terzo in conformità di un accordo internazionale sono esclusi dall'ambito di applicazione della presente direttiva. La presente direttiva non si applica alle missioni diplomatiche e consolari degli Stati membri nei paesi terzi né ai loro sistemi informatici e di rete, nella misura in cui tali sistemi siano situati nei locali della missione o utilizzati per utenti in un paese terzo.

(9) Gli Stati membri dovrebbero essere in grado di adottare le misure necessarie a garantire la tutela degli interessi essenziali della sicurezza nazionale, a salvaguardare l'ordine pubblico e la pubblica sicurezza e a consentire la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati. A tal fine, gli Stati membri dovrebbero poter esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati da determinati obblighi previsti dalla presente direttiva per quanto riguarda tali attività. Qualora un soggetto fornisca servizi esclusivamente a un ente della pubblica amministrazione escluso dall'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero poter esentare tale soggetto da determinati obblighi stabiliti dalla presente direttiva per quanto riguarda tali servizi. Inoltre, nessuno Stato membro dovrebbe essere tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza. Dovrebbero essere prese in considerazione in tale contesto le norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP. Il protocollo TLP deve essere inteso come uno strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i team di risposta agli incidenti di sicurezza informatica (CSIRT) e in alcuni centri di analisi e condivisione delle informazioni.

(10) Sebbene la presente direttiva si applichi ai soggetti che svolgono attività di produzione di energia elettrica da centrali nucleari, alcune di tali attività possono essere collegate alla sicurezza nazionale. In tal caso, uno Stato membro dovrebbe poter esercitare la propria responsabilità per la salvaguardia della propria sicurezza nazionale in relazione a tali attività, comprese le attività all'interno della catena del valore nucleare, conformemente ai trattati.

(11) Alcuni soggetti svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati, fornendo nel contempo anche servizi fiduciari. I prestatori di servizi fiduciari che rientrano nell'ambito di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([6]) dovrebbero rientrare nell'ambito di applicazione della presente direttiva al fine di garantire un livello di requisiti di sicurezza e supervisione analogo a quello precedentemente stabilito in tale regolamento nei confronti dei prestatori di servizi fiduciari. In linea con l'esclusione di alcuni servizi specifici dal regolamento (UE) n. 910/2014, la presente direttiva non dovrebbe applicarsi alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

([6]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

(12) I fornitori di servizi postali come definiti dalla direttiva 97/67/CE del Parlamento europeo e del Consiglio ([7]), inclusi i fornitori di servizi di corriere, dovrebbero essere soggetti alla presente direttiva se provvedono ad almeno una delle fasi della catena di consegna postale, in particolare la raccolta, lo smistamento, il trasporto o la distribuzione di invii postali, compresi i servizi di ritiro, tenendo conto nel contempo del grado di relativa dipendenza dai sistemi informatici e di rete. I servizi di trasporto che non sono forniti nell'ambito di una di tali fasi dovrebbero essere esclusi dall'ambito di applicazione dei servizi postali.

(13) Data l'intensificazione e la crescente sofisticazione delle minacce informatiche, gli Stati membri dovrebbero adoperarsi per garantire che i soggetti esclusi dall'ambito di applicazione della presente direttiva raggiungano un livello elevato di cibersicurezza e sostengano l'attuazione di misure equivalenti di gestione dei rischi di cibersicurezza, che riflettano la natura sensibile di tali soggetti.

(14) A qualsiasi trattamento di dati personali ai sensi della presente direttiva si applica il diritto dell'Unione in materia di protezione dei dati personali e della vita privata. La presente direttiva non pregiudica in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([8]) e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([9]). La presente direttiva non dovrebbe pertanto pregiudicare, tra l'altro, i compiti e i poteri delle autorità competenti di monitorare il rispetto del diritto dell'Unione in vigore in materia di protezione dei dati personali e della vita privata.

(15) I soggetti che rientrano nell'ambito di applicazione della presente direttiva ai fini del rispetto delle misure di gestione dei rischi di cibersicurezza e degli obblighi di segnalazione dovrebbero essere classificati in due categorie, essenziali e importanti, in funzione della loro importanza per il settore o il tipo di servizi che forniscono, nonché delle loro dimensioni. A tale riguardo, si dovrebbe tenere debitamente conto, se del caso, di tutte le valutazioni settoriali dei rischi o di tutti gli orientamenti pertinenti elaborati dalle autorità competenti. I regimi di esecuzione e di vigilanza per tali due categorie di soggetti dovrebbero essere differenziati per garantire un giusto equilibrio tra i requisiti e gli obblighi basati sui rischi, da un lato, e gli oneri amministrativi derivanti dalla vigilanza della conformità, dall'altro.

(16) Al fine di evitare che soggetti che hanno imprese partner o che sono imprese collegate siano considerati soggetti essenziali o importanti qualora ciò sarebbe sproporzionato, gli Stati membri possono tenere conto del grado di indipendenza di cui gode un soggetto in relazione alle sue imprese partner e collegate nell'applicazione dell'articolo 6, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE. In particolare, gli Stati membri possono tenere conto del fatto che un soggetto è indipendente dalle sue imprese partner o collegate in termini di sistemi informatici e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce. Su tale base, se del caso, gli Stati membri possono ritenere che tale soggetto non sia considerato una media impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, o non superi i massimali per le medie imprese di cui al paragrafo 1 di tale articolo se, tenuto conto del grado di indipendenza di tale soggetto, si ritenga che esso non sia consideri una media impresa o superi tali massimali nel caso in cui siano stati presi in considerazione solo i suoi dati. Ciò lascia impregiudicati gli obblighi di cui alla presente direttiva per le imprese associate e collegate che rientrano nel campo di applicazione della presente direttiva.

(17) Gli Stati membri dovrebbero poter decidere che i soggetti definiti, prima dell'entrata in vigore della presente direttiva, come operatori di servizi essenziali ai sensi della direttiva (UE) 2016/1148 debbano essere considerati soggetti essenziali.

([7]) Direttiva 97/67/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e il miglioramento della qualità del servizio (GU L 15 del 21.1.1998, pag. 14).

([8]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([9]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

(18) Al fine di garantire una panoramica chiara dei soggetti che rientrano nell'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero definire un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. A tal fine, gli Stati membri dovrebbero imporre ai soggetti di trasmettere alle autorità competenti almeno le seguenti informazioni, vale a dire il nome, l'indirizzo e i recapiti aggiornati, compresi gli indirizzi di posta elettronica, le serie IP e i numeri di telefono del soggetto, se del caso, il settore e il sottosettore pertinente di cui agli allegati e, ove applicabile, un elenco degli Stati membri in cui prestano servizi che rientrano nell'ambito di applicazione della presente direttiva. A tal fine, la Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), dovrebbe fornire senza indebito ritardo orientamenti e modelli relativi all'obbligo di fornire informazioni. Per facilitare la compilazione e l'aggiornamento dell'elenco dei soggetti essenziali e importanti, nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, gli Stati membri dovrebbero poter istituire meccanismi nazionali che consentano ai soggetti di registrarsi. Qualora esistano registri a livello nazionale, gli Stati membri possono decidere in merito ai meccanismi appropriati che consentono di identificare i soggetti che rientrano nell'ambito di applicazione della presente direttiva.

(19) Gli Stati membri dovrebbero essere tenuti a comunicare alla Commissione almeno il numero di soggetti essenziali e importanti per ciascun settore e sottosettore di cui agli allegati, nonché le informazioni pertinenti sul numero di soggetti identificati e sulla disposizione, tra quelle previste dalla presente direttiva, sulla base della quale sono stati identificati, e la tipologia dei servizi che forniscono. Gli Stati membri sono incoraggiati a scambiare con la Commissione informazioni sui soggetti essenziali e importanti e, in caso di incidente di cibersicurezza su vasta scala, informazioni pertinenti quali il nome del soggetto interessato.

(20) La Commissione, in collaborazione con il gruppo di cooperazione e previa consultazione dei pertinenti portatori di interessi, dovrebbe fornire orientamenti relativi all'attuazione dei criteri applicabili alle microimprese e alle piccole imprese per valutare se rientrino nell'ambito di applicazione della presente direttiva. La Commissione dovrebbe inoltre garantire che vengano forniti orientamenti adeguati alle microimprese e alle piccole imprese rientranti nell'ambito di applicazione della presente direttiva. La Commissione, con il sostegno degli Stati membri, dovrebbe fornire alle microimprese e alle piccole imprese informazioni al riguardo.

(21) La Commissione potrebbe fornire orientamenti volti ad assistere gli Stati membri nell'attuazione delle disposizioni della presente direttiva sull'ambito di applicazione e nella valutazione della proporzionalità delle misure da adottare ai sensi della presente direttiva, segnatamente per quanto riguarda i soggetti con modelli di business o contesti operativi complessi, in base ai quali un soggetto può soddisfare contemporaneamente i criteri assegnati ai soggetti essenziali e importanti o può svolgere simultaneamente attività che rientrano in parte nell'ambito di applicazione della presente direttiva e in parte ne sono escluse.

(22) La presente direttiva stabilisce lo scenario di riferimento per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione in tutti i settori che rientrano nel suo ambito di applicazione. Al fine di evitare la frammentazione delle disposizioni in materia di cibersicurezza contenute negli atti giuridici dell'Unione, allorché ulteriori atti giuridici settoriali dell'Unione relativi alle misure di gestione dei rischi di cibersicurezza e agli obblighi di segnalazione siano ritenuti necessari per garantire un elevato livello di cibersicurezza in tutta l'Unione, la Commissione dovrebbe valutare se tali ulteriori disposizioni possano essere stabilite in un atto di esecuzione ai sensi della presente direttiva. Qualora tali atti di esecuzione non siano adeguati a detto scopo, gli atti giuridici settoriali dell'Unione potrebbero contribuire a garantire un livello elevato di cibersicurezza in tutta l'Unione, tenendo pienamente conto delle specificità e delle complessità dei settori interessati. A tal fine, la presente direttiva non preclude l'adozione di ulteriori atti giuridici settoriali dell'Unione riguardanti le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione che tengano debitamente conto della necessità di un quadro di sicurezza informatica globale e coerente. La presente direttiva lascia impregiudicate le competenze di esecuzione esistenti conferite alla Commissione in una serie di settori, tra cui i trasporti e l'energia.

(23) Qualora un atto giuridico settoriale dell'Unione faccia obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare incidenti significativi, e nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, tali disposizioni, comprese

quelle relative alla vigilanza e all'esecuzione, si applicano a detti soggetti. Qualora un atto giuridico settoriale dell'Unione non contempli tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva dovrebbero continuare ad applicarsi ai soggetti non contemplati da tale atto.

(24) Qualora le disposizioni di un atto giuridico settoriale dell'Unione impongano ai soggetti essenziali o importanti di rispettare gli obblighi di effetto almeno equivalente agli obblighi di segnalazione di cui alla presente direttiva, è opportuno garantire la coerenza e l'efficacia del trattamento delle notifiche degli incidenti. A tal fine, le disposizioni in materia di notifica degli incidenti dell'atto giuridico settoriale dell'Unione dovrebbero fornire ai CSIRT, alle autorità competenti o ai punti di contatto unici di cui alla presente direttiva un accesso immediato alle notifiche degli incidenti di cibersicurezza (punti di contatto unici) presentate in conformità dell'atto giuridico settoriale dell'Unione. In particolare, tale accesso immediato può essere garantito se le notifiche degli incidenti sono trasmesse senza indebito ritardo al CSIRT, all'autorità competente o al punto di contatto unico ai sensi della presente direttiva. Se del caso, gli Stati membri dovrebbero istituire un meccanismo di segnalazione automatica e diretta, che garantisca la condivisione sistematica e immediata delle informazioni con i CSIRT, le autorità competenti o il punto di contatto unico per quanto riguarda la gestione di tali notifiche di incidenti. Al fine di semplificare la comunicazione e di attuare il meccanismo di segnalazione automatica e diretta, gli Stati membri potrebbero, conformemente all'atto giuridico settoriale dell'Unione, utilizzare un punto di accesso unico.

(25) Gli atti giuridici settoriali dell'Unione che prevedono misure di gestione dei rischi di cibersicurezza o obblighi di segnalazione di effetto almeno equivalente a quelli stabiliti nella presente direttiva potrebbero prevedere che le autorità competenti ai sensi di tali atti esercitino i loro poteri di vigilanza ed esecuzione in relazione a tali misure o obblighi con l'assistenza delle autorità competenti ai sensi della presente direttiva. Le autorità competenti interessate potrebbero stabilire modalità di cooperazione a tale scopo. Tali modalità di cooperazione potrebbero precisare, tra l'altro, le procedure relative al coordinamento delle attività di vigilanza, tra cui le procedure di indagine e di ispezione in loco conformemente al diritto nazionale e un meccanismo per lo scambio di informazioni pertinenti in materia di vigilanza ed esecuzione tra autorità competenti, compreso l'accesso alle informazioni relative alla cibersicurezza richieste dalle autorità competenti ai sensi della presente direttiva.

(26) Qualora atti giuridici settoriali dell'Unione impongano o forniscano incentivi a soggetti affinché notifichino minacce informatiche significative, gli Stati membri dovrebbero altresì incoraggiare la condivisione di minacce informatiche significative con i CSIRT, le autorità competenti o i punti di contatto unici ai sensi della presente direttiva, al fine di garantire un maggiore livello di consapevolezza di tali organismi in merito al panorama delle minacce informatiche e consentire loro di rispondere in modo efficace e tempestivo qualora tali minacce si concretizzino.

(27) I futuri atti giuridici settoriali dell'Unione dovrebbero tenere debitamente conto delle definizioni e del quadro di vigilanza e applicazione previsto dalla presente direttiva.

(28) Il regolamento UE 2022/2554 del Parlamento europeo e del Consiglio ([10]) dovrebbe essere considerato un atto giuridico settoriale dell'Unione in relazione alla presente direttiva per quanto riguarda i soggetti del settore finanziario. Invece delle disposizioni stabilite nella presente direttiva dovrebbero applicarsi quelle del regolamento (UE) 2022/2554 relative alle misure di gestione del rischio relativo alle tecnologie dell'informazione e della comunicazione (TIC), alla gestione degli incidenti relativi alle TIC e, in particolare, alla segnalazione degli incidenti gravi relativi alle TIC, nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e ai rischi di terze parti relativi alle TIC. Gli Stati membri non dovrebbero pertanto applicare le disposizioni della presente direttiva riguardanti gli obblighi di gestione e segnalazione dei rischi di cibersicurezza e la vigilanza e l'esecuzione ai soggetti finanziari contemplati dal regolamento (UE) 2022/2554 Al tempo stesso è importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario a norma della presente direttiva. A tal fine, il regolamento (UE) 2022/2554 consente alle autorità europee di vigilanza (AEV) e alle autorità competenti a norma di tale regolamento di partecipare alle attività del gruppo di cooperazione, di scambiare informazioni e cooperare con i punti di contatto unici, nonché con i CSIRT e le autorità competenti ai sensi della presente direttiva. Le autorità competenti a norma del regolamento (UE) 2022/2554 dovrebbero inoltre trasmettere

([10]) 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 (Cfr. pag. 1 della presente Gazzetta ufficiale).

i dettagli degli incidenti più gravi connessi alle TIC e, se del caso, delle minacce informatiche significative ai CSIRT, alle autorità competenti o ai punti di contatto unici nazionali a norma della presente direttiva. Ciò è possibile fornendo accesso immediato alle notifiche di incidenti e la loro trasmissione diretta o attraverso un unico punto di accesso. Gli Stati membri dovrebbero inoltre continuare a includere il settore finanziario nelle loro strategie di cibersicurezza e i CSIRT nazionali possono contemplare il settore finanziario nelle loro attività.

(29) Al fine di evitare lacune o duplicazioni per quanto riguarda gli obblighi di cibersicurezza imposti ai soggetti del settore dell'aviazione, le autorità nazionali designate a norma dei regolamenti (CE) n. 300/2008 ([11]) e (UE) 2018/1139 ([12]) del Parlamento europeo e del Consiglio e le autorità competenti a norma della presente direttiva dovrebbero cooperare in relazione all'attuazione delle misure di gestione dei rischi di cibersicurezza e alla vigilanza della conformità con tali misure a livello nazionale. La conformità di un soggetto con i requisiti di sicurezza di cui ai regolamenti (CE) n. 300/2008 e (UE) 2018/1139 e ai pertinenti atti delegati e di esecuzione adottati a norma di tali regolamenti potrebbe essere considerata dalle autorità competenti ai sensi della presente direttiva una conformità ai corrispondenti requisiti di cui alla presente direttiva.

(30) In considerazione delle interconnessioni tra la cibersicurezza e la sicurezza fisica dei soggetti, dovrebbe essere garantito un approccio coerente tra la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio ([13]) e la presente direttiva. A tal fine, i soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557 dovrebbero essere considerati soggetti essenziali a norma della presente direttiva. Inoltre, ciascuno Stato membro dovrebbe provvedere affinché la propria strategia nazionale in materia di cibersicurezza preveda un quadro strategico per il rafforzamento del coordinamento all'interno di detto Stato membro tra le proprie autorità competenti a norma della presente direttiva e quelle previste dalla direttiva (UE) 2022/2557 nel contesto della condivisione delle informazioni sui rischi, sulle minacce informatiche e sugli incidenti nonché sui rischi, sulle minacce e sugli incidenti non informatici e dello svolgimento di compiti di vigilanza. Le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 dovrebbero cooperare e scambiarsi informazioni senza indebito ritardo, in particolare per quanto riguarda l'individuazione dei soggetti critici, delle minacce informatiche, dei rischi e degli incidenti nonché per quanto riguarda i rischi, le minacce e gli incidenti non informatici che interessano i soggetti critici, tra cui le misure di cibersicurezza e fisiche adottate dai soggetti critici nonché i risultati delle attività di vigilanza svolte riguardo a tali soggetti.

Inoltre, al fine di razionalizzare le attività di vigilanza tra le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 e di ridurre al minimo gli oneri amministrativi per i soggetti interessati, tali autorità competenti dovrebbero adoperarsi per armonizzare i modelli di notifica degli incidenti e le procedure di vigilanza. Se del caso, le autorità competenti a norma della direttiva (UE) 2022/2557 dovrebbero poter chiedere alle autorità competenti ai sensi della presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557 A tal fine, le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 dovrebbero cooperare e scambiarsi informazioni, ove possibile in tempo reale.

(31) I soggetti appartenenti al settore delle infrastrutture digitali sono essenzialmente basati su sistemi informatici e di rete e pertanto gli obblighi loro imposti a norma della presente direttiva dovrebbero riguardare in modo globale la sicurezza fisica di tali sistemi nell'ambito delle loro misure di gestione dei rischi di cibersicurezza e obblighi di segnalazione. Poiché tali materie sono disciplinate dalla presente direttiva, gli obblighi di cui ai capi III, IV e VI della direttiva (UE) 2022/2557 non si applicano a detti soggetti.

([11]) Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

([12]) Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

([13]) Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE (cfr. pag. 164 della presente Gazzetta ufficiale).

(32) Sostenere e preservare un sistema dei nomi di dominio affidabile, resiliente e sicuro sono fattori chiave per mantenere l'integrità di internet e sono essenziali per il suo funzionamento costante e stabile, da cui dipendono l'economia e la società digitali. La presente direttiva dovrebbe applicarsi ai server dei nomi di dominio di primo livello (*top level domain* — TLD) e ai fornitori di servizi DNS che si intendono come soggetti che forniscono servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet o ai servizi di risoluzione autorevoli dei nomi di dominio. La presente direttiva non dovrebbe applicarsi ai server dei nomi radice (*root name server*).

(33) I servizi di cloud computing dovrebbero comprendere servizi digitali che consentono l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche quando tali risorse sono distribuite in varie ubicazioni. Le risorse di calcolo comprendono risorse come reti, server o altre infrastrutture, sistemi operativi, software, archiviazione, applicazioni e servizi. I modelli di servizio del cloud computing comprendono, tra gli altri, il servizio a livello di infrastruttura (IaaS), il servizio a livello di piattaforma (PaaS), il servizio a livello di software (SaaS) e il servizio a livello di rete (NaaS). I modelli di distribuzione del cloud computing dovrebbero comprendere il cloud privato, di comunità, pubblico e ibrido. I servizi di cloud computing e di distribuzione hanno lo stesso significato dei termini di servizio e dei modelli di distribuzione di cui alla norma ISO/IEC 17788:2014. La capacità dell'utente di cloud computing di provvedere unilateralmente all'autofornitura di capacità di calcolo, come il tempo di utilizzo di un server o lo spazio di archiviazione in rete, senza alcuna interazione umana da parte del fornitore di servizi di cloud computing potrebbe essere descritta come «amministrazione su richiesta».

L'espressione «ampio accesso remoto» (*broad network access*) è utilizzata per descrivere il fatto che le capacità cloud sono fornite sulla rete e accessibili attraverso meccanismi che promuovono l'uso di piattaforme client eterogenee leggere o pesanti (compresi telefoni cellulari, tablet, computer portatili e workstation). Il termine «scalabile» si riferisce alle risorse informatiche che sono assegnate in modo flessibile dal fornitore di servizi nel cloud, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione «pool elastico» è usata per descrivere le risorse di calcolo fornite e rilasciate in base alla domanda, al fine di aumentare e diminuire rapidamente le risorse disponibili in base al carico di lavoro. Il termine «condivisibile» è usato per descrivere le risorse di calcolo che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre l'elaborazione è effettuata separatamente per ciascun utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica. Il termine «distribuito» è usato per descrivere le risorse di calcolo che si trovano su diversi computer o dispositivi collegati in rete e che comunicano e si coordinano tra di loro mediante il passaggio di messaggi.

(34) Dato l'emergere di tecnologie innovative e di nuovi modelli di business, si prevede che compariranno sul mercato interno nuovi modelli di servizio e di distribuzione del cloud computing in risposta all'evoluzione delle esigenze dei clienti. In tale contesto, i servizi di cloud computing possono essere forniti in una forma altamente distribuita, anche più vicina al luogo in cui i dati vengono generati o raccolti, passando così dal modello tradizionale a un modello altamente distribuito (*edge computing*).

(35) È possibile che i servizi offerti dai fornitori di servizi di data center non siano sempre forniti sotto forma di servizi di cloud computing. È pertanto possibile che i data center non facciano sempre parte dell'infrastruttura di cloud computing. Al fine di gestire tutti i rischi posti alla sicurezza dei sistemi informatici e di rete, la presente direttiva dovrebbe pertanto applicarsi ai fornitori di servizi di data center che non sono servizi di cloud computing. Ai fini della presente direttiva, il termine «servizio di data center» dovrebbe applicarsi alla fornitura di un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale. Il termine «servizio di data center» non si dovrebbe applicare ai data center interni e aziendali posseduti e gestiti per fini propri dal soggetto interessato.

(36) Le attività di ricerca svolgono un ruolo fondamentale nello sviluppo di nuovi prodotti e processi. Molte di tali attività sono svolte da soggetti che condividono, diffondono o sfruttano i risultati della loro ricerca per scopi commerciali. Tali soggetti possono pertanto essere attori importanti nelle catene del valore, il che rende la sicurezza dei loro sistemi informatici e di rete parte integrante della cibersicurezza globale del mercato interno. Gli organismi di ricerca dovrebbero essere intesi come soggetti che concentrano la parte essenziale delle loro attività sullo

svolgimento di ricerca applicata o sviluppo sperimentale, ai sensi del Manuale di Frascati 2015 dell'Organizzazione per la cooperazione e lo sviluppo economici: «Linee guida per la raccolta e la trasmissione di dati sulla ricerca e lo sviluppo sperimentale», al fine di sfruttarne i risultati a fini commerciali quali la produzione o lo sviluppo di un prodotto o di un processo, la prestazione di un servizio, o la loro commercializzazione.

(37) Le crescenti interdipendenze sono il risultato di una rete di fornitura di servizi sempre più transfrontaliera e interdipendente che utilizza infrastrutture chiave in tutta l'Unione in settori quali quelli dell'energia, dei trasporti, delle infrastrutture digitali, delle acque potabili e reflue, della sanità, di determinati aspetti della pubblica amministrazione, nonché dello spazio, per quanto riguarda la fornitura di determinati servizi che dipendono da infrastrutture di terra possedute, gestite e utilizzate dagli Stati membri o da soggetti privati, ad esclusione, pertanto, delle infrastrutture possedute, gestite o utilizzate dall'Unione o per suo conto nell'ambito del suo programma spaziale. Tali interdipendenze implicano che qualsiasi perturbazione, anche se inizialmente limitata a un soggetto o a un settore, possa avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata sulla fornitura di servizi in tutto il mercato interno. Gli attacchi informatici intensificatisi durante la pandemia di COVID-19 hanno mostrato la vulnerabilità di società sempre più interdipendenti di fronte a rischi di bassa probabilità.

(38) In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali già esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione, è opportuno che gli Stati membri abbiano la facoltà di designare o istituire una o più autorità nazionali competenti responsabili per la cibersicurezza e per i compiti di supervisione ai sensi della presente direttiva.

(39) Al fine di agevolare la cooperazione e la comunicazione transfrontaliere tra autorità e permettere che la presente direttiva sia attuata efficacemente, è necessario che ogni Stato membro designi un punto di contatto unico nazionale incaricato di coordinare le questioni relative alla sicurezza dei sistemi informatici e di rete e la cooperazione transfrontaliera a livello dell'Unione.

(40) I punti di contatto unici dovrebbero garantire un'efficace cooperazione transfrontaliera con le autorità competenti di altri Stati membri e, se del caso, con la Commissione e l'ENISA. I punti di contatto unici dovrebbero pertanto essere incaricati di trasmettere le notifiche di incidenti significativi con impatto transfrontaliero ai punti di contatto unici degli altri Stati membri interessati, su richiesta del CSIRT o dell'autorità competente. A livello nazionale, i punti di contatto unici dovrebbero consentire un'agevole cooperazione intersettoriale con le altre autorità competenti. I punti di contatto unici potrebbero anche ricevere dalle autorità competenti, a norma del regolamento (UE) 2022/2554, le pertinenti informazioni sugli incidenti riguardanti i soggetti del settore finanziario, che essi dovrebbero poter trasmettere, a seconda dei casi, ai CSIRT o alle autorità competenti a norma della presente direttiva.

(41) Gli Stati membri dovrebbero essere adeguatamente dotati delle capacità tecniche e organizzative necessarie a prevenire e rilevare gli incidenti e i rischi, nonché a rispondervi e a mitigare il loro impatto. Gli Stati membri dovrebbero pertanto designare uno o più CSIRT ai sensi della presente direttiva e garantire che essi dispongano di risorse e capacità tecniche adeguate. I CSIRT dovrebbero rispondere ai requisiti stabiliti nella presente direttiva al fine di garantire l'esistenza di capacità efficaci e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione. Gli Stati membri dovrebbero poter designare come CSIRT le squadre di pronto intervento informatico (CERT) esistenti. Al fine di rafforzare il rapporto di fiducia tra i soggetti e i CSIRT, nei casi in cui un CSIRT faccia parte di un'autorità competente, gli Stati membri dovrebbero poter prendere in considerazione la separazione funzionale tra i compiti operativi svolti dai CSIRT, in particolare per quanto riguarda la condivisione delle informazioni e l'assistenza fornita ai soggetti, e le attività di vigilanza delle autorità competenti.

(42) I CSIRT sono incaricati della gestione degli incidenti. Ciò comprende il trattamento di grandi volumi di dati talvolta sensibili. Gli Stati membri dovrebbero garantire che i CSIRT dispongano di un'infrastruttura per la condivisione e il trattamento delle informazioni, nonché di personale ben attrezzato, che garantisca la riservatezza e l'affidabilità delle loro operazioni. I CSIRT potrebbero anche adottare codici di condotta a tale riguardo.

(43) Per quanto riguarda i dati personali, i CSIRT dovrebbero poter fornire, in conformità del regolamento (UE) 2016/679, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete utilizzati per la fornitura dei servizi del soggetto. Se del caso, gli Stati membri dovrebbero mirare a garantire un pari livello di capacità tecniche per tutti i CSIRT settoriali. Gli Stati membri dovrebbero poter chiedere l'assistenza dell'ENISA nello sviluppo di CSIRT nazionali.

(44) I CSIRT dovrebbero avere la capacità, su richiesta di un soggetto essenziale o importante, di monitorare le risorse di quest'ultimo connesse a internet, sia in loco che a distanza, per identificare, comprendere e gestire i rischi organizzativi generali del soggetto con riguardo alle compromissioni della catena di approvvigionamento individuate di recente o le vulnerabilità critiche. Il soggetto dovrebbe essere incoraggiato a comunicare al CSIRT se gestisce un'interfaccia gestionale privilegiata, poiché ciò potrebbe incidere sulla velocità delle azioni di mitigazione.

(45) Data l'importanza della cooperazione internazionale in materia di cibersicurezza, i CSIRT dovrebbero poter partecipare a reti di cooperazione internazionale, oltre alla rete di CSIRT istituita dalla presente direttiva. Pertanto, ai fini dello svolgimento dei loro compiti, i CSIRT e le autorità competenti dovrebbero poter scambiare informazioni, compresi i dati personali, con team nazionali di risposta agli incidenti per la sicurezza informatica o autorità competenti di paesi terzi, purché siano soddisfatte le condizioni previste dal diritto dell'Unione in materia di protezione dei dati per i trasferimenti di dati personali verso paesi terzi, tra cui quelle a norma dell'articolo 49 del regolamento (UE) 2016/679.

(46) È essenziale garantire risorse adeguate per il conseguimento degli obiettivi della presente direttiva e consentire alle autorità competenti e ai CSIRT di lo svolgimento dei compiti ivi stabiliti. Gli Stati membri possono introdurre a livello nazionale un meccanismo di finanziamento per coprire le spese necessarie in relazione allo svolgimento dei compiti degli enti pubblici responsabili della cibersicurezza nello Stato membro ai sensi della presente direttiva. Tale meccanismo dovrebbe essere conforme al diritto dell'Unione, essere proporzionato e non discriminatorio e dovrebbe tenere conto dei diversi approcci nella fornitura di servizi sicuri.

(47) La rete di CSIRT dovrebbe continuare a contribuire al rafforzamento della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri. Al fine di rafforzare la cooperazione operativa a livello di Unione, la rete di CSIRT dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali Europol.

(48) Al fine di conseguire e mantenere un livello elevato di cibersicurezza, le strategie nazionali per la cibersicurezza richieste dalla presente direttiva dovrebbero comprendere quadri coerenti che forniscano obiettivi e priorità strategici nel settore della cibersicurezza e la governance per conseguirli. Tali strategie possono essere rappresentate da uno o più strumenti legislativi o non legislativi.

(49) Le politiche di igiene informatica (*cyber hygiene*) pongono le fondamenta per la protezione delle infrastrutture delle reti e dei sistemi di informazione, dell'hardware, del software e della sicurezza delle applicazioni online, nonché dei dati aziendali o degli utenti finali su cui si basano i soggetti. Le politiche di igiene informatica, che comprendono uno scenario di riferimento comune delle prassi, tra cui gli aggiornamenti del software e dell'hardware, i cambi di password, la gestione delle nuove installazioni, la limitazione degli account di accesso a livello di amministratore e il backup dei dati, consentono un quadro proattivo di preparazione e sicurezza e protezione generale in caso di incidenti o minacce informatiche. L'ENISA dovrebbe monitorare e analizzare le politiche di igiene informatica degli Stati membri.

(50) La consapevolezza in materia di cibersicurezza e l'igiene informatica sono essenziali per migliorare il livello di cibersicurezza all'interno dell'Unione, in particolare alla luce del crescente numero di dispositivi connessi sempre più utilizzati negli attacchi informatici. È opportuno adoperarsi per migliorare la consapevolezza generale dei rischi connessi a tali dispositivi; al contempo, valutazioni a livello di Unione potrebbero contribuire a garantire una comprensione comune di tali rischi nel mercato interno.

(51) Gli Stati membri dovrebbero incoraggiare l'uso di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici, consentendo di destinare in modo più efficace risorse per affrontare gli attacchi informatici. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cibersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli strumenti automatizzati o semiautomatizzati nella cibersicurezza, e, se del caso, la condivisione dei dati necessari per formare gli utenti di tali tecnologie e migliorarle. L'utilizzo di tutte le tecnologie innovative, compresa l'intelligenza artificiale, dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, compresi i principi di protezione dei dati con riguardo all'accuratezza, alla minimizzazione dei dati, all'equità e alla trasparenza, nonché alla sicurezza dei dati, come la più recente crittografia. I requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679 dovrebbero essere pienamente rispettati.

(52) Gli strumenti e le applicazioni di cibersicurezza open source possono contribuire a un livello più elevato di apertura e avere un impatto positivo sull'efficienza dell'innovazione industriale. Gli standard aperti facilitano l'interoperabilità tra gli strumenti di sicurezza, a vantaggio della sicurezza dei portatori di interessi industriali. Gli strumenti e le applicazioni open source in materia di cibersicurezza possono mobilitare la più ampia comunità di sviluppatori, consentendo la diversificazione dei fornitori. Una fonte aperta può portare a un processo di verifica più trasparente degli strumenti connessi alla cibersicurezza e a un processo di individuazione delle vulnerabilità guidato dalla comunità. Gli Stati membri dovrebbero pertanto poter promuovere l'utilizzo di software open source e standard aperti, perseguendo politiche relative all'uso di dati aperti e open source come parte della sicurezza attraverso la trasparenza. Le politiche che promuovono l'introduzione e l'uso sostenibile di strumenti di sicurezza informatica open source rivestono particolare importanza per le piccole e medie imprese che devono sostenere notevoli costi per l'attuazione, e che potrebbero essere minimizzati riducendo la necessità di applicazioni o strumenti specifici.

(53) I servizi pubblici sono sempre più collegati alle reti digitali nelle città per migliorare le reti di trasporto urbano, l'approvvigionamento idrico e gli impianti di smaltimento dei rifiuti, nonché aumentare l'efficienza dell'illuminazione e del riscaldamento degli edifici. Tali servizi pubblici digitali sono vulnerabili agli attacchi informatici e corrono il rischio, in caso di successo di un attacco informatico, di danneggiare i cittadini su larga scala a causa della loro interconnessione. Gli Stati membri dovrebbero elaborare una politica che affronti lo sviluppo di tali città connesse o intelligenti, così come i loro potenziali effetti sulla società, nell'ambito della loro strategia nazionale per la cibersicurezza.

(54) Negli ultimi anni l'Unione ha dovuto far fronte a un aumento esponenziale di attacchi ransomware, in cui i malware criptano dati e sistemi e chiedono il pagamento di un riscatto per il rilascio. La frequenza e la gravità crescenti degli attacchi ransomware possono essere determinate da diversi fattori, come i diversi modelli di attacco, i modelli criminali commerciali che considerano il «ransomware come un servizio» e le criptovalute, le richieste di riscatto e l'aumento degli attacchi contro la catena di approvvigionamento. Gli Stati membri dovrebbero sviluppare politiche, come parte delle loro strategie nazionali per la cibersicurezza, che affrontino l'aumento degli attacchi ransomware.

(55) I partenariati pubblico-privato (PPP) nell'ambito della cibersicurezza possono fornire il quadro appropriato per lo scambio di conoscenze, la condivisione delle migliori pratiche e la creazione di un livello comune di comprensione tra i portatori di interessi. Gli Stati membri dovrebbero promuovere politiche che sostengano l'istituzione di PPP specifici della cibersicurezza. Tali politiche dovrebbero chiarire, tra l'altro, l'ambito di applicazione e i portatori di interessi coinvolti, il modello di governance, le opzioni di finanziamento disponibili e l'interazione tra i portatori di interessi partecipanti con riguardo ai PPP. I PPP possono sfruttare le competenze dei soggetti del settore privato per assistere le autorità competenti nello sviluppo di servizi e processi all'avanguardia, compresi, lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza.

(56) Gli Stati membri dovrebbero, nelle loro strategie nazionali per la cibersicurezza, rispondere alle esigenze specifiche in materia di cibersicurezza delle piccole e medie imprese. Le piccole e medie imprese rappresentano nell'Unione, un'ampia percentuale del mercato industriale e commerciale e spesso faticano ad adattarsi alle nuove pratiche commerciali in un mondo sempre più connesso e all'ambiente digitale, con dipendenti che lavorano da casa e imprese che sono gestite in misura crescente online. Alcune piccole e medie imprese si confrontano con sfide specifiche in materia di cibersicurezza, come la scarsa consapevolezza informatica, la mancanza di sicurezza informatica a distanza, l'elevato costo delle soluzioni di cibersicurezza e l'aumento del livello di minaccia, dovuto ad esempio ai ransomware, aspetti in relazione ai quali dovrebbero ricevere linee guida e assistenza. Le piccole e medie imprese stanno diventando sempre di più il bersaglio di attacchi nella catena di approvvigionamento a causa delle loro misure meno rigorose di gestione del rischio di cibersicurezza e di gestione degli attacchi, nonché della limitata disponibilità di risorse destinate alla sicurezza. Tali attacchi della catena di approvvigionamento non solo hanno un

impatto sulle piccole e medie imprese e sulle loro operazioni isolatamente, ma possono anche avere un effetto a cascata su attacchi più gravi nei confronti di soggetti di cui sono fornitori. Gli Stati membri dovrebbero, attraverso le loro strategie nazionali in materia di cibersicurezza, aiutare le piccole e medie imprese fronteggiare le sfide a cui sono sottoposte nelle loro catene di approvvigionamento. Gli Stati membri dovrebbero disporre di un punto di contatto per le piccole e medie imprese a livello nazionale o regionale, che fornisca linee guida e assistenza alle piccole e medie imprese, o le diriga verso gli organismi appropriati per l'orientamento e l'assistenza in materia di cibersicurezza. Gli Stati membri sono altresì incoraggiati a offrire servizi come la configurazione e la registrazione di siti internet, che abilitino le microimprese e le piccole imprese che non dispongono di tali capacità.

(57) Gli Stati membri dovrebbero adottare politiche volte a promuovere la protezione informatica attiva nell'ambito delle loro strategie nazionali per la cibersicurezza, come parte di una strategia difensiva più ampia. Anziché reagire, la protezione informatica attiva consiste nel prevenire, individuare, monitorare, analizzare e attenuare in maniera attiva le violazioni della sicurezza della rete, in combinazione con il ricorso a capacità predisposte all'interno e all'esterno della rete vittima. Ciò potrebbe includere l'offerta da parte degli Stati membri di servizi o strumenti gratuiti a determinati soggetti, tra cui controlli self-service, strumenti di rilevamento e servizi di rimozione. La capacità di condividere e comprendere in modo rapido e automatico informazioni e analisi riguardanti le minacce, segnalazioni di attività informatiche e azioni di risposta è fondamentale per consentire un'unità di sforzi al fine di prevenire, individuare, affrontare e bloccare con successo gli attacchi informatici nei confronti dei sistemi informatici e di rete. La protezione informatica attiva si basa su una strategia difensiva, che esclude misure offensive.

(58) Poiché lo sfruttamento delle vulnerabilità nei sistemi informatici e di rete può causare perturbazioni e danni significativi, la rapida individuazione e correzione di tali vulnerabilità è un fattore importante per la riduzione dei rischi. I soggetti che sviluppano o amministrano tali sistemi informatici e di rete dovrebbero pertanto stabilire procedure adeguate per gestire le vulnerabilità nel momento in cui vengono scoperte. Poiché le vulnerabilità sono spesso rilevate e divulgate da terzi, il fabbricante o fornitore di prodotti TIC o servizi TIC dovrebbe anche mettere in atto le procedure necessarie per ricevere informazioni sulla vulnerabilità da terzi. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC 29147 forniscono orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. Al fine di facilitare il contesto della divulgazione volontaria delle vulnerabilità, è particolarmente importante rafforzare il coordinamento tra persone fisiche e giuridiche segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. La divulgazione coordinata delle vulnerabilità dovrebbe comprendere anche il coordinamento tra la persona fisica o giuridica segnalante e il fabbricante o il fornitore di prodotti TIC o servizi TIC potenzialmente vulnerabili, per quanto riguarda i tempi per la risoluzione e la pubblicazione delle vulnerabilità.

(59) La Commissione, l'ENISA e gli Stati membri dovrebbero continuare a promuovere gli allineamenti agli standard internazionali e alle migliori prassi industriali esistenti nel settore della gestione dei rischi, ad esempio nei settori delle valutazioni della sicurezza della catena di approvvigionamento, della condivisione delle informazioni e della divulgazione delle vulnerabilità.

(60) Gli Stati membri, in cooperazione con l'ENISA, dovrebbero adottare misure volte a facilitare la divulgazione coordinata delle vulnerabilità stabilendo una politica nazionale pertinente. Nell'ambito di tale politica nazionale, gli Stati membri dovrebbero mirare ad affrontare, nella misura del possibile, le sfide incontrate dagli esperti che fanno ricerca sulle vulnerabilità, compresa la loro potenziale esposizione alla responsabilità penale, conformemente al diritto nazionale. Dato che in alcuni Stati membri le persone fisiche e giuridiche che fanno ricerca sulle vulnerabilità potrebbero essere esposte alla responsabilità penale e civile, gli Stati membri sono incoraggiati ad adottare linee guida per quanto riguarda la non perseguibilità dei ricercatori in materia di sicurezza delle informazioni e l'esenzione dalla responsabilità civile per le loro attività.

(61) Gli Stati membri dovrebbero designare un CSIRT come coordinatore, che funga da intermediario di fiducia tra le persone fisiche o giuridiche segnalanti e i fabbricanti o fornitori di prodotti TIC o servizi TIC suscettibili di essere interessati dalle vulnerabilità, ove necessario. I compiti del CSIRT designato come coordinatore dovrebbero comprendere in particolare l'individuazione e il contatto dei soggetti interessati, l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità

che interessano più soggetti (divulgazione multilaterale coordinata di vulnerabilità). Qualora la vulnerabilità segnalata possa avere un impatto significativo su soggetti in più di uno Stato membro, i CSIRT designati come coordinatori dovrebbero cooperare nell'ambito della rete CSIRT, se del caso.

(62) L'accesso a informazioni corrette e tempestive sulle vulnerabilità che interessano i prodotti TIC e i servizi TIC contribuisce a una migliore gestione dei rischi di cibersicurezza. Le fonti di informazioni pubblicamente disponibili sulle vulnerabilità sono uno strumento importante per i soggetti e gli utenti dei loro servizi, ma anche per le autorità competenti e i CSIRT. Per tale motivo l'ENISA dovrebbe istituire una banca dati europea delle vulnerabilità in cui i soggetti, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione della presente direttiva, e i loro fornitori di sistemi informatici e di rete, così come le autorità competenti e i CSIRT, possano, su base volontaria, divulgare le vulnerabilità e fornire informazioni su di esse che consentano agli utenti di adottare adeguate misure di attenuazione. Lo scopo di tale banca dati è far fronte alle sfide uniche poste dai rischi per i soggetti unionali. Inoltre, l'ENISA dovrebbe istituire una procedura adeguata relativamente al processo di pubblicazione, al fine di dare ai soggetti il tempo di adottare misure di attenuazione per quanto riguarda le loro vulnerabilità e utilizzare le più avanzate misure di gestione dei rischi sulla cibersicurezza, nonché le serie di dati leggibili meccanicamente e le corrispondenti interfacce. Per incoraggiare una cultura della divulgazione delle vulnerabilità, la divulgazione non dovrebbe andare a scapito della persona fisica o giuridica segnalante.

(63) Sebbene simili registri o banche dati delle vulnerabilità esistano già, questi sono ospitati e mantenuti da soggetti non stabiliti nell'Unione. Una banca dati europea delle vulnerabilità mantenuta dall'ENISA garantirebbe una maggiore trasparenza, per quanto riguarda la procedura di pubblicazione prima della divulgazione al pubblico della vulnerabilità, e resilienza in caso di perturbazioni o interruzioni nella fornitura di servizi analoghi. Per evitare la duplicazione degli sforzi e perseguire, nella misura del possibile, la complementarità, l'ENISA dovrebbe valutare la possibilità di concludere accordi di cooperazione strutturata con registri simili o banche dati di competenza di giurisdizioni di paesi terzi. In particolare, l'ENISA dovrebbe valutare la possibilità di una stretta cooperazione con gli operatori del sistema delle vulnerabilità e delle esposizioni comuni (CVE).

(64) Il gruppo di cooperazione dovrebbe sostenere e agevolare la cooperazione strategica e lo scambio di informazioni, come anche rafforzare la fiducia tra gli Stati membri. Il gruppo di cooperazione dovrebbe stabilire un programma di lavoro ogni due anni. Il programma di lavoro dovrebbe comprendere le azioni che il gruppo di cooperazione deve intraprendere per attuare i suoi obiettivi e compiti. Il calendario per la definizione del primo programma di lavoro adottato a norma della presente direttiva dovrebbe essere allineato a quello dell'ultimo programma di lavoro definito a norma della direttiva (UE) 2016/1148, al fine di evitare eventuali perturbazioni nel lavoro del gruppo di cooperazione.

(65) Nello sviluppo delle linee guida, il gruppo di cooperazione dovrebbe coerentemente mappare le soluzioni e le esperienze nazionali, valutare l'impatto dei risultati del gruppo di cooperazione per quanto riguarda gli approcci nazionali, discutere le sfide in materia di attuazione e formulare raccomandazioni specifiche, in particolare per quanto riguarda l'agevolazione di un allineamento nel recepimento della presente direttiva tra gli Stati membri, da realizzare attraverso una migliore attuazione delle norme esistenti. Il gruppo di cooperazione potrebbe anche mappare le soluzioni nazionali al fine di promuovere la compatibilità delle soluzioni di cibersicurezza applicate a ciascun settore specifico in tutta l'Unione. Ciò è particolarmente pertinente per i settori che hanno natura internazionale e transfrontaliera.

(66) Il gruppo di cooperazione dovrebbe rimanere un forum flessibile ed essere in grado di reagire alle nuove e mutevoli priorità strategiche e alle sfide, tenendo conto nel contempo della disponibilità di risorse. Esso potrebbe organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere dati e contributi sulle sfide strategiche emergenti. Inoltre, il gruppo di cooperazione dovrebbe effettuare una valutazione periodica dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware. Al fine di rafforzare la cooperazione a livello di Unione, il gruppo di cooperazione dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori le

pertinenti istituzioni, organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali il Parlamento europeo, Europol, il Comitato europeo per la protezione dei dati, l'Agenzia dell'Unione europea per la sicurezza aerea, istituita con il regolamento (UE) 2018/1139 e l'Agenzia dell'Unione europea per il programma spaziale, istituita con il regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio ([14]).

(67) Le autorità competenti e i CSIRT dovrebbero poter partecipare a programmi di scambio per funzionari di altri Stati membri, nell'ambito di un quadro specifico e, se del caso, previo il nulla osta di sicurezza necessario per i funzionari che partecipano a tali programmi di scambio, al fine di migliorare la cooperazione e rafforzare la fiducia tra gli Stati membri. Le autorità competenti dovrebbero adottare le misure necessarie per consentire a funzionari di altri Stati membri di svolgere un ruolo efficace nelle attività dell'autorità competente ospitante o del CSIRT ospitante.

(68) Gli Stati membri dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE, di cui alla raccomandazione (UE) 2017/1584 della Commissione ([15]), attraverso le reti di cooperazione esistenti, in particolare la rete europea di collegamento per le crisi informatiche (EU-CyCLONe), la rete di CSIRT e il gruppo di cooperazione. EU-CyCLONe e la rete di CSIRT dovrebbero cooperare sulla base di disposizioni procedurali che specifichino i dettagli di tale cooperazione ed evitare duplicazioni dei compiti. Il regolamento interno di EU-CyCLONe dovrebbe specificare ulteriormente i meccanismi di funzionamento della rete, compresi i ruoli, i mezzi di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione. Per la gestione delle crisi a livello dell'Unione, le parti pertinenti dovrebbero affidarsi ai dispositivi integrati dell'UE per la risposta politica alle crisi nel quadro della decisione di esecuzione (UE) 2018/1993 del Consiglio ([16]) (dispositivi IPCR). A tal fine la Commissione dovrebbe far ricorso al processo di coordinamento intersettoriale delle crisi ad alto livello del sistema ARGUS. Se la crisi implica un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune dovrebbe essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna.

(69) Conformemente all'allegato della raccomandazione (UE) 2017/1584, per incidente di cibersicurezza su vasta scala si intende un incidente di cibersicurezza che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi, o che ha un impatto significativo su almeno due Stati membri. A seconda della loro causa e del loro impatto, gli incidenti di cibersicurezza su vasta scala possono aggravarsi e trasformarsi in vere e proprie crisi che non consentono il corretto funzionamento del mercato interno, o che comportano gravi rischi di pubblica sicurezza in diversi Stati membri o nell'intera Unione. Data l'ampia portata e, nella maggior parte dei casi, la natura transfrontaliera di tali incidenti, gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'Unione dovrebbero cooperare a livello tecnico, operativo e politico per coordinare adeguatamente la risposta in tutta l'Unione.

(70) Gli incidenti e le crisi di cibersicurezza su vasta scala a livello dell'Unione richiedono un'azione coordinata per garantire una risposta rapida ed efficace, a causa dell'elevato grado di interdipendenza tra settori e Stati membri. La disponibilità di sistemi informatici e di rete ciberresilienti e la disponibilità, la riservatezza e l'integrità dei dati sono essenziali per la sicurezza dell'Unione e per la protezione dei suoi cittadini, delle sue imprese e delle sue istituzioni da incidenti e minacce informatiche, nonché per rafforzare la fiducia delle persone e delle organizzazioni nella capacità dell'Unione di promuovere e proteggere un ciberspazio globale, aperto, libero, stabile e sicuro basato sui diritti umani, le libertà fondamentali, la democrazia e lo Stato di diritto.

([14]) Regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e che abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE (GU L 170 del 12.5.2021, pag. 69).

([15]) Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

([16]) Decisione di esecuzione (UE) 2018/1993 del Consiglio, dell'11 dicembre 2018, relativa ai dispositivi integrati dell'UE per la risposta politica alle crisi (GU L 320 del 17.12.2018, pag. 28).

(71) EU-CyCLONe dovrebbe fungere da intermediario tra il livello tecnico e politico durante gli incidenti e le crisi di cibersicurezza su vasta scala e dovrebbe rafforzare la cooperazione a livello operativo e sostenere il processo decisionale a livello politico. In cooperazione con la Commissione, tenuto conto della competenza di quest'ultima nel settore della gestione delle crisi, EU-CyCLONe dovrebbe basarsi sui risultati della rete di CSIRT e utilizzare le proprie capacità per elaborare analisi d'impatto di incidenti e crisi di cibersicurezza su vasta scala.

(72) Gli attacchi informatici sono di natura transfrontaliera e un incidente significativo può perturbare e danneggiare le infrastrutture informatiche critiche da cui dipende il corretto funzionamento del mercato interno. La raccomandazione (UE) 2017/1584 tratta il ruolo di tutti i soggetti interessati. Inoltre, la Commissione è responsabile, nel quadro del meccanismo unionale di protezione civile istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([17]), delle azioni di preparazione generali, che comprendono la gestione del Centro di coordinamento della risposta alle emergenze e del sistema comune di comunicazione e di informazione in caso di emergenza, il mantenimento e l'ulteriore sviluppo della consapevolezza situazionale e delle capacità di analisi, nonché la predisposizione e la gestione della capacità di mobilitare e inviare squadre di esperti in caso di richiesta di assistenza da parte di uno Stato membro o di un paese terzo. La Commissione è inoltre responsabile di fornire relazioni analitiche per i dispositivi IPCR nel quadro della decisione di esecuzione (UE) 2018/1993, anche in relazione alla consapevolezza situazionale e alla preparazione in materia di cibersicurezza, come anche per la consapevolezza situazionale e la risposta alle crisi nei settori dell'agricoltura, delle condizioni meteorologiche avverse, della mappatura e delle previsioni dei conflitti, dei sistemi di allarme rapido in caso di catastrofi naturali, delle emergenze sanitarie, della sorveglianza delle malattie infettive, della salute delle piante, degli incidenti chimici, della sicurezza di alimenti e mangimi, della salute degli animali, della migrazione, delle dogane, delle emergenze radiologiche e nucleari, e dell'energia.

(73) Ove opportuno, l'Unione può concludere accordi internazionali, in conformità all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi dovrebbero garantire gli interessi dell'Unione e un'adeguata protezione dei dati. Ciò non dovrebbe escludere il diritto degli Stati membri di cooperare con paesi terzi sulla gestione delle vulnerabilità e la gestione dei rischi di cibersicurezza, agevolando la segnalazione e la condivisione delle informazioni generali in conformità al diritto dell'Unione.

(74) Al fine di facilitare l'effettiva attuazione della presente direttiva per quanto riguarda, tra l'altro, la gestione delle vulnerabilità, le misure di gestione dei rischi di cibersicurezza, gli obblighi di segnalazione e gli accordi di condivisione delle informazioni relative alla cibersicurezza, gli Stati membri possono cooperare con i paesi terzi e intraprendere attività ritenute appropriate a tal fine, tra cui scambi di informazioni relative a minacce informatiche, incidenti, vulnerabilità, strumenti e metodi, tattiche, tecniche e procedure, preparazione ed esercitazioni in materia di gestione delle crisi informatiche, formazioni, instaurazione di un clima di fiducia e accordi strutturati di condivisione delle informazioni.

(75) Dovrebbero essere introdotte revisioni tra pari per contribuire a trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca e conseguire un livello comune elevato di cibersicurezza. Le revisioni tra pari possono portare a idee e raccomandazioni preziose che rafforzano le capacità globali in materia di cibersicurezza, creando un altro percorso funzionale per la condivisione delle migliori pratiche tra gli Stati membri e contribuendo a migliorare i livelli di maturità degli Stati membri in materia di cibersicurezza. Inoltre, le revisioni tra pari dovrebbero tenere conto dei risultati di meccanismi analoghi, come il sistema di revisione tra pari della rete di CSIRT e dovrebbero apportare un valore aggiunto ed evitare duplicazioni. L'attuazione delle revisioni tra pari dovrebbe lasciare impregiudicato il diritto dell'Unione o nazionale in materia di protezione delle informazioni riservate o classificate.

(76) Il gruppo di cooperazione dovrebbe stabilire una metodologia di autovalutazione per gli Stati membri, al fine di coprire fattori quali il livello di attuazione delle misure di gestione dei rischi di cibersicurezza e degli obblighi di segnalazione, il livello di capacità e l'efficacia dell'esercizio dei compiti delle autorità competenti, le capacità operative dei CSIRT, il livello di attuazione dell'assistenza reciproca, il livello di attuazione degli accordi di condivisione delle informazioni in materia di cibersicurezza o questioni specifiche di natura transfrontaliera o intersettoriale. Gli Stati membri dovrebbero essere incoraggiati ad effettuare autovalutazioni su base regolare e a presentare e discutere i risultati della loro autovalutazione nell'ambito del gruppo di cooperazione.

([17]) Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).

(77) La responsabilità di garantire la sicurezza dei sistemi informatici e di rete incombe in larga misura a soggetti essenziali e importanti. È opportuno promuovere e sviluppare una cultura della gestione dei rischi, che comprenda valutazioni dei rischi e l'attuazione di misure di gestione dei rischi di cibersicurezza adeguate ai rischi esistenti.

(78) Le misure di gestione dei rischi dovrebbero tenere conto del grado di dipendenza del soggetto essenziale o importante dai sistemi informatici e di rete e comprendere misure per individuare eventuali rischi di incidenti, per prevenire e rilevare incidenti, nonché per rispondervi, riprendersi da essi e attenuarne l'impatto. La sicurezza dei sistemi informatici e di rete dovrebbe comprendere la sicurezza dei dati conservati, trasmessi e elaborati. Le misure di gestione dei rischi di cibersicurezza dovrebbero prevedere un'analisi sistemica, tenendo conto del fattore umano, onde avere un quadro completo della sicurezza del sistema informatico e di rete.

(79) Poiché le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, le misure di gestione dei rischi di cibersicurezza dovrebbero essere basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi. Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000. A tale riguardo, i soggetti essenziali e importanti dovrebbero altresì, nell'ambito delle loro misure di gestione dei rischi di cibersicurezza, affrontare la questione della sicurezza delle risorse umane e disporre di strategie adeguate di controllo dell'accesso. Tali misure dovrebbero essere coerenti con la direttiva (UE) 2022/2557.

(80) Al fine di dimostrare la conformità alle misure di gestione dei rischi di cibersicurezza e in mancanza di adeguati sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([18]), gli Stati membri, in consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, dovrebbero promuovere l'uso delle pertinenti norme europee e internazionali da parte dei soggetti essenziali e importanti o possono imporre a questi ultimi di utilizzare prodotti TIC, servizi TIC e processi TIC certificati.

(81) Per evitare di imporre un onere finanziario e amministrativo sproporzionato ai soggetti essenziali e importanti, le misure di gestione dei rischi di cibersicurezza dovrebbero essere proporzionate ai rischi posti al sistema informatico e di rete interessato, tenendo conto dello stato dell'arte di tali misure e, se del caso, di pertinenti norme europee e internazionali, come anche dei relativi costi di attuazione.

(82) Le misure di gestione dei rischi di cibersicurezza dovrebbero essere proporzionate al grado di esposizione del soggetto essenziali o importanti ai rischi e all'impatto sociale ed economico che un incidente avrebbe. Nel definire misure di gestione dei rischi di cibersicurezza adattate ai soggetti essenziali e importanti, è opportuno tenere debitamente conto dell'esposizione al rischio divergente dei soggetti essenziali e importanti, quali la criticità del soggetto, i rischi, compresi i rischi sociali, cui è esposto, le dimensioni del soggetto e la probabilità del verificarsi di incidenti e la loro gravità, compreso il loro impatto sociale ed economico.

([18]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersicurezza) (GU L 151 del 7.6.2019, pag. 15).

(83) I soggetti essenziali e importanti dovrebbero garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività. Si tratta in particolare di sistemi informatici e di rete privati gestiti dal personale informatico interno dei soggetti essenziali e importanti oppure la cui sicurezza sia stata esternalizzata. Le misure di gestione e gli obblighi di segnalazione dei rischi di cibersicurezza stabiliti nella presente direttiva dovrebbero applicarsi ai pertinenti soggetti essenziali e importanti indipendentemente dal fatto che tali soggetti effettuino internamente la manutenzione dei loro sistemi informatici e di rete o che la esternalizzino.

(84) Tenuto conto della loro natura transfrontaliera, i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, e i fornitori di servizi di sicurezza gestiti e i prestatori di servizi fiduciari dovrebbero essere soggetti a un elevato livello di armonizzazione a livello dell'Unione. L'attuazione delle misure di gestione del rischio di cibersicurezza con riguardo a tali soggetti dovrebbe pertanto essere agevolata da un atto di esecuzione.

(85) Affrontare i rischi derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori, ad esempio i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti e gli editori di software, è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono stati vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti essenziali e importanti dovrebbero pertanto valutare e tenere in considerazione la qualità e la resilienza complessive dei prodotti e dei servizi, delle misure di gestione dei rischi di cibersicurezza in essi integrate e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. In particolare, i soggetti essenziali e importanti dovrebbero essere incoraggiati a integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali con i loro fornitori e fornitori di servizi diretti. Tali soggetti potrebbero prendere in considerazione i rischi derivanti da altri livelli di fornitori e fornitori di servizi.

(86) Tra i fornitori di servizi, i fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. I fornitori di servizi di sicurezza gestiti sono stati tuttavia essi stessi bersaglio di attacchi informatici e, a causa della loro stretta integrazione nelle attività dei soggetti, presentano un particolare rischio. I soggetti essenziali e importanti dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti.

(87) Nell'ambito dei loro compiti di vigilanza, le autorità competenti possono inoltre beneficiare di servizi di cibersicurezza quali gli audit sulla sicurezza, i test di penetrazione o la risposta agli incidenti.

(88) I soggetti essenziali e importanti dovrebbero inoltre affrontare i rischi derivanti dalle loro interazioni e relazioni con altri portatori di interessi nell'ambito di un ecosistema più ampio, anche per quanto riguarda la lotta contro lo spionaggio industriale e la tutela dei segreti commerciali. In particolare, tali soggetti dovrebbero adottare misure adeguate per garantire che la loro cooperazione con gli istituti accademici e di ricerca avvenga in linea con le loro politiche in materia di cibersicurezza e segua le buone pratiche per quanto riguarda l'accesso sicuro e la diffusione delle informazioni in generale e la tutela della proprietà intellettuale in particolare. Analogamente, data l'importanza e il valore dei dati per le attività dei soggetti essenziali e importanti, tali soggetti dovrebbero adottare tutte le opportune misure di gestione dei rischi di cibersicurezza quando si affidano ai servizi di trasformazione e analisi dei dati forniti da terzi.

(89) I soggetti essenziali e importanti dovrebbero adottare un'ampia gamma di pratiche di igiene informatica di base quali principi zero trust, aggiornamenti del software, configurazione dei dispositivi, segmentazione della rete, gestione dell'identità e dell'accesso o sensibilizzazione degli utenti, organizzare per il loro personale una formazione e sensibilizzarlo alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersicurezza e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersicurezza quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informatici e di rete.

(90) Per affrontare ulteriormente i principali rischi relativi alla catena di approvvigionamento e aiutare i soggetti essenziali e importanti che operano nei settori disciplinati dalla presente direttiva a gestire adeguatamente i rischi connessi alla catena di approvvigionamento e ai fornitori, il gruppo di cooperazione, in cooperazione con la Commissione e l'ENISA e, se del caso, previa consultazione dei pertinenti portatori di interessi compresi quelli del settore, dovrebbe effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche, come è avvenuto per le reti 5G in seguito alla raccomandazione (UE) 2019/534 della Commissione ([19]), al fine di individuare, per settore, i servizi TIC, i sistemi TIC o i prodotti TIC critici e le minacce e le vulnerabilità pertinenti. Dette valutazioni coordinate dei rischi per la sicurezza dovrebbero individuare le misure, i piani di attenuazione e le migliori pratiche per contrastare le dipendenze critiche, i potenziali singoli punti di vulnerabilità, le minacce, le vulnerabilità e gli altri rischi associati alla catena di approvvigionamento, ed esplorare modalità per incoraggiare ulteriormente una loro più ampia adozione da parte dei soggetti essenziali e importanti. I potenziali fattori di rischio non tecnici, come l'indebita influenza di un paese terzo sui fornitori e i fornitori di servizi, in particolare nel caso di modelli alternativi di governance, includono vulnerabilità nascoste o backdoor e potenziali turbative sistemiche dell'approvvigionamento, segnatamente in caso di lock-in tecnologico o di dipendenza dal fornitore.

(91) Le valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche, alla luce delle caratteristiche del settore interessato, dovrebbero tenere conto dei fattori tecnici e, se opportuno, non tecnici, compresi quelli definiti nella raccomandazione (UE) 2019/534, nella valutazione dei rischi coordinata dell'UE della cibersicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione. Per individuare le catene di approvvigionamento che dovrebbero essere soggette a una valutazione coordinata dei rischi per la sicurezza, dovrebbero essere presi in considerazione i seguenti criteri: i) la misura in cui i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi TIC, sistemi TIC o prodotti TIC critici; ii) la pertinenza di specifici servizi TIC, sistemi TIC o prodotti TIC critici per lo svolgimento di funzioni critiche o sensibili, compreso il trattamento dei dati personali; iii) la disponibilità di servizi TIC, sistemi TIC o prodotti TIC alternativi; iv) la resilienza dell'intera catena di approvvigionamento di servizi TIC, sistemi TIC o prodotti TIC, durante tutto il loro ciclo di vita, contro eventi perturbatori e v) per i servizi TIC, sistemi TIC o prodotti TIC emergenti, la loro potenziale importanza futura per le attività dei soggetti. Inoltre, si dovrebbe porre un accento particolare sui servizi TIC, i sistemi TIC o i prodotti TIC che sono soggetti a requisiti specifici derivanti da paesi terzi.

(92) Al fine di semplificare gli obblighi imposti ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico e ai prestatori di servizi fiduciari relativi alla sicurezza dei loro sistemi informatici e di rete, nonché di consentire a tali soggetti e alle autorità competenti ai sensi, rispettivamente, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio ([20]) e del regolamento (UE) n. 910/2014 di beneficiare del quadro giuridico istituito dalla presente direttiva, comprese la designazione di un CSIRT responsabile della gestione degli incidenti, la partecipazione delle autorità competenti interessate alle attività del gruppo di cooperazione e della rete di CSIRT, tali soggetti dovrebbero rientrare nell'ambito di applicazione della presente direttiva. Le corrispondenti disposizioni stabilite nel regolamento (UE) n. 910/2014 e nella direttiva (UE) 2018/1972 relative all'imposizione di obblighi di sicurezza e notifica a queste tipologie di soggetti dovrebbero pertanto essere soppresse. Le norme relative agli obblighi di segnalazione stabilite nella presente direttiva dovrebbero lasciare impregiudicati il regolamento (UE) 2016/679 e la direttiva 2002/58/CE.

(93) Gli obblighi in materia di cibersicurezza stabiliti nella presente direttiva dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n. 910/2014. È opportuno chiedere ai prestatori di servizi fiduciari di adottare tutte le misure adeguate e proporzionate per gestire i rischi posti ai loro servizi, anche in relazione ai clienti e ai terzi che vi fanno affidamento, nonché di segnalare gli incidenti a norma della presente direttiva. Tali obblighi in materia di cibersicurezza e segnalazione dovrebbero riguardare anche la protezione fisica dei servizi forniti. I requisiti per i prestatori di servizi fiduciari qualificati stabiliti all'articolo 24 del regolamento (UE) n. 910/2014 continuano ad applicarsi.

([19]) Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G (GU L 88 del 29.3.2019, pag. 42).

([20]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

(94) Gli Stati membri possono conferire il ruolo di autorità competenti per i servizi fiduciari agli organismi di vigilanza a norma del regolamento (UE) n. 910/2014 al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite con l'applicazione di detto regolamento. In tal caso, le autorità competenti a norma della presente direttiva dovrebbero cooperare strettamente e in modo tempestivo con tali organismi di vigilanza scambiando le informazioni pertinenti al fine di assicurare l'efficace vigilanza dei prestatori di servizi fiduciari nonché l'effettivo rispetto, da parte di questi ultimi, delle prescrizioni stabilite nella presente direttiva e nel regolamento (UE) n. 910/2014. Se del caso, il CSIRT o l'autorità competente a norma della presente direttiva dovrebbero informare immediatamente l'organismo di vigilanza a norma del regolamento (UE) n. 910/2014 di qualunque minaccia informatica o incidente significativi notificati aventi un impatto sui servizi fiduciari nonché di qualunque violazione, da parte di un prestatore di servizi fiduciari, della presente direttiva. Ai fini della segnalazione, gli Stati membri possono, se del caso, utilizzare il punto di ingresso unico stabilito per effettuare segnalazioni comuni e automatiche di incidenti destinate sia all'organismo di vigilanza a norma del regolamento (UE) n. 910/2014 sia al CSIRT o all'autorità competente a norma della presente direttiva.

(95) Se opportuno e per evitare inutili perturbazioni, gli orientamenti nazionali esistenti adottati per il recepimento delle norme relative alle misure di sicurezza di cui agli articoli 40 e 41 della direttiva (UE) 2018/1972 dovrebbero essere presi in considerazione nel recepimento della presente direttiva, basandosi quindi sulle conoscenze e competenze già acquisite nell'ambito della direttiva (UE) 2018/1972 per quanto riguarda le misure di sicurezza e le notifiche degli incidenti. L'ENISA può inoltre elaborare orientamenti sui requisiti di sicurezza e sugli obblighi di segnalazione per i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico al fine di facilitare l'armonizzazione e la transizione e di ridurre al minimo le perturbazioni. Gli Stati membri possono conferire il ruolo di autorità competenti per le comunicazioni elettroniche alle autorità nazionali di regolamentazione ai sensi della direttiva (UE) 2018/1972 al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite a seguito con l'attuazione di tale direttiva.

(96) Vista la crescente importanza dei servizi di comunicazione interpersonale indipendenti dal numero quali definiti nella direttiva (UE) 2018/1972, è necessario assicurare che anche tali servizi siano soggetti ad adeguati requisiti di sicurezza in considerazione della loro specificità e della loro rilevanza economica. Dal momento che la superficie di attacco continua ad ampliarsi, i servizi di comunicazione interpersonale indipendenti dal numero, come i servizi di messaggistica, stanno diventando vettori di attacco diffusi. I responsabili di atti malevoli utilizzano piattaforme per comunicare e indurre le vittime ad aprire pagine web compromesse, aumentando così la probabilità di incidenti che interessano lo sfruttamento dei dati personali e, per estensione, la sicurezza dei sistemi informatici e di rete. I fornitori di servizi di comunicazione interpersonale indipendenti dal numero dovrebbero garantire un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Dato che i fornitori di servizi di comunicazione interpersonale indipendenti dal numero solitamente non esercitano un controllo effettivo sulla trasmissione dei segnali sulle reti, il grado di rischio per tali servizi può essere considerato, per certi aspetti, inferiore a quello dei servizi di comunicazione elettronica tradizionali. Lo stesso vale per i servizi di comunicazione interpersonale quali definiti nella direttiva (UE) 2018/1972 che utilizzano numeri e che non esercitano un controllo effettivo sulla trasmissione dei segnali.

(97) Il mercato interno dipende più che mai dal funzionamento di internet. I servizi di quasi tutti i soggetti essenziali e importanti dipendono dai servizi forniti via internet. Al fine di garantire l'erogazione senza intoppi dei servizi forniti dai soggetti essenziali e importanti, è fondamentale che tutti i fornitori di reti pubbliche di comunicazione elettronica dispongano di adeguate misure di gestione dei rischi di cibersicurezza e segnalino gli incidenti significativi connessi. Gli Stati membri dovrebbero garantire il mantenimento della sicurezza delle reti pubbliche di comunicazione elettronica e la protezione dei loro interessi vitali in materia di sicurezza contro il sabotaggio e lo spionaggio. Poiché la connettività internazionale migliora e accelera la digitalizzazione competitiva dell'Unione e della sua economia, gli incidenti che interessano i cavi di comunicazione sottomarini dovrebbero essere segnalati al CSIRT o, se del caso, all'autorità competente. La strategia nazionale per la cibersicurezza dovrebbe, se del caso, tenere conto della cibersicurezza dei cavi di comunicazione sottomarini e includere una mappatura dei potenziali rischi di cibersicurezza e misure di attenuazione per garantire il massimo livello di protezione.

(98) Al fine di salvaguardare la sicurezza delle reti pubbliche di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico, l'uso delle tecnologie di cifratura, in particolare la cifratura end-to-end, come anche concetti di sicurezza incentrati sui dati, quali la cartografia, la segmentazione, la marcatura, la politica di accesso e la gestione dell'accesso, nonché le decisioni di accesso automatizzato, dovrebbe essere promosso. Ove necessario, l'uso della cifratura, in particolare la cifratura end-to-end, dovrebbe essere reso obbligatorio per i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, conformemente ai principi di sicurezza e tutela della vita privata per impostazione predefinita e fin dalla progettazione ai fini della presente direttiva. L'uso della cifratura end-to-end dovrebbe essere conciliato con i poteri degli Stati membri di garantire la tutela della sicurezza pubblica e dei loro interessi essenziali in materia di sicurezza, nonché di consentire la prevenzione, l'indagine, l'accertamento e il perseguimento di reati in conformità al diritto dell'Unione. Tuttavia, ciò non dovrebbe indebolire la cifratura end-to-end, che è una tecnologia fondamentale per un'efficace protezione dei dati, della privacy e della sicurezza delle comunicazioni.

(99) Al fine di salvaguardare la sicurezza, e prevenire abusi e manipolazioni, delle reti pubbliche di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico, è opportuno promuovere il ricorso a standard in materia di inoltro sicuro per garantire l'integrità e la solidità delle funzioni di inoltro in tutto l'ecosistema dei fornitori di servizi di accesso a internet.

(100) Al fine di salvaguardare la funzionalità e l'integrità di internet e promuovere la sicurezza e la resilienza del DNS, i portatori di interessi pertinenti, tra cui soggetti del settore privato dell'Unione, fornitori di servizi di comunicazione elettronica accessibili al pubblico, in particolare fornitori di servizi di accesso a internet e fornitori di motori di ricerca online, dovrebbero essere incoraggiati ad adottare una strategia di diversificazione della risoluzione DNS. Inoltre, gli Stati membri dovrebbero incoraggiare lo sviluppo e l'utilizzo di un servizio europeo di risoluzione DNS pubblico e sicuro.

(101) La presente direttiva stabilisce un approccio in più fasi alla segnalazione degli incidenti significativi al fine di trovare il giusto equilibrio tra, da un lato, una segnalazione rapida che contribuisca ad attenuare la potenziale diffusione di incidenti e consenta ai soggetti essenziali e importanti di chiedere assistenza e, dall'altro, una segnalazione approfondita che tragga insegnamenti preziosi dai singoli incidenti e migliori nel tempo la resilienza informatica dei singoli soggetti e di interi settori. A tale proposito, la presente direttiva dovrebbe includere la segnalazione di incidenti che, sulla base di una valutazione iniziale condotta dal soggetto interessato, potrebbero causare gravi perturbazioni operative dei servizi o perdite finanziarie per tale soggetto, o interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali. Detta valutazione iniziale dovrebbe tenere conto, tra l'altro, dei sistemi informatici e di rete interessati, in particolare della loro importanza nella fornitura dei servizi del soggetto, della gravità e delle caratteristiche tecniche di una minaccia informatica e delle eventuali vulnerabilità sottostanti che vengono sfruttate, nonché dell'esperienza del soggetto in caso di incidenti simili. Indicatori quali la misura in cui il funzionamento del servizio è interessato, la durata di un incidente o il numero di destinatari dei servizi interessati potrebbero svolgere un ruolo importante nel determinare se la perturbazione operativa del servizio è grave.

(102) Qualora vengano a conoscenza di un incidente significativo, i soggetti essenziali o importanti dovrebbero essere tenuti a presentare un preallarme senza indebito ritardo, e comunque entro 24 ore. Tale preallarme dovrebbe essere seguito da una notifica dell'incidente. I soggetti interessati dovrebbero presentare una notifica dell'incidente senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, allo scopo, in particolare, di aggiornare le informazioni trasmesse nel preallarme e di indicare una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione. Una relazione finale dovrebbe essere presentata entro un mese dalla notifica dell'incidente. Il preallarme dovrebbe contenere soltanto le informazioni necessarie per informare il CSIRT, o se del caso l'autorità competente, dell'incidente significativo e consentire al soggetto interessato di chiedere assistenza, se necessario. Tale preallarme dovrebbe indicare, ove opportuno, se l'incidente significativo è sospettato di essere il risultato di atti illeciti o malevoli e se è probabile che abbia un impatto transfrontaliero. Gli Stati membri dovrebbero garantire che l'obbligo di presentare tale preallarme, o la successiva notifica dell'incidente, non sottragga le risorse del soggetto notificante alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie, per evitare che gli obblighi di segnalazione degli incidenti sottraggano risorse alla gestione della risposta agli incidenti o

compromettano altrimenti gli sforzi dei soggetti a tale riguardo. In caso di incidente in corso al momento della trasmissione della relazione finale, gli Stati membri dovrebbero provvedere affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente significativo.

(103) Se del caso, i soggetti essenziali e importanti dovrebbero comunicare senza indebito ritardo ai destinatari dei loro servizi le misure o le azioni correttive che possono adottare per attenuare i rischi che derivano da una minaccia informatica significativa. Tali soggetti dovrebbero, ove opportuno e in particolare quando è probabile che la minaccia informatica significativa si concretizzi, informare i destinatari dei loro servizi anche in merito alla minaccia stessa. L'obbligo di informare tali destinatari in merito alle minacce informatiche significative dovrebbe essere soddisfatto con la massima diligenza possibile, ma non dovrebbe esonerare tali soggetti dall'obbligo di adottare, a proprie spese, provvedimenti adeguati e immediati per prevenire eventuali minacce di questo tipo o porvi rimedio e ristabilire il normale livello di sicurezza del servizio. La fornitura ai destinatari dei servizi di tali informazioni riguardanti le minacce informatiche significative dovrebbe essere gratuita e avvenire in una lingua facilmente comprensibile.

(104) I fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico dovrebbero attuare la sicurezza fin dalla progettazione e per impostazione predefinita e informare i destinatari dei loro servizi di minacce informatiche significative e delle misure che questi ultimi possono adottare per proteggere la sicurezza dei loro dispositivi e delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecnologie di cifratura.

(105) Un approccio proattivo alle minacce informatiche è una componente essenziale delle misure di gestione dei rischi di cibersicurezza che dovrebbe consentire alle autorità competenti di impedire efficacemente che le minacce informatiche si trasformino in incidenti che possono causare danni materiali o immateriali considerevoli. A tal fine, la notifica di minacce informatiche riveste un'importanza fondamentale. I soggetti sono pertanto incoraggiati a segnalare su base volontaria le minacce informatiche.

(106) Al fine di semplificare la comunicazione delle informazioni richieste a norma della presente direttiva e di ridurre gli oneri amministrativi per i soggetti, gli Stati membri dovrebbero fornire mezzi tecnici quali un punto di ingresso unico, sistemi automatizzati, moduli online, interfacce di facile utilizzo, modelli e piattaforme dedicate per l'uso dei soggetti, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione della presente direttiva, per la comunicazione delle pertinenti informazioni da segnalare. I finanziamenti dell'Unione a sostegno dell'attuazione della presente direttiva, in particolare nell'ambito del programma Europa digitale istituito dal regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio ([21]), potrebbero includere il sostegno a punti di ingresso unici. Inoltre, i soggetti si trovano spesso in una situazione in cui un particolare incidente, a causa delle sue caratteristiche, deve essere segnalato a varie autorità in conseguenza degli obblighi di notifica previsti da vari strumenti giuridici. Tali casi creano ulteriori oneri amministrativi e potrebbero anche generare incertezze in merito al formato e alle procedure di tali notifiche. Qualora sia istituito un punto di ingresso unico, gli Stati membri sono incoraggiati a utilizzare tale punto di ingresso anche per le notifiche degli incidenti di sicurezza previste da altre normative dell'Unione, quali il regolamento (UE) 2016/679 e la direttiva 2002/58/CE. L'uso di tale punto di accesso unico per la segnalazione di incidenti di sicurezza a norma del regolamento (UE) 2016/679 e della direttiva 2002/58/CE non dovrebbe pregiudicare l'applicazione delle disposizioni di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE, in particolare quelle relative all'indipendenza delle autorità ivi menzionate. L'ENISA, in collaborazione con il gruppo di cooperazione, dovrebbe elaborare modelli comuni di notifica mediante orientamenti per semplificare e razionalizzare le informazioni da segnalare richieste a norma del diritto dell'Unione e ridurre gli oneri amministrativi per i soggetti notificanti.

(107) Se si sospetta che un incidente sia connesso ad attività criminali gravi a norma del diritto dell'Unione o nazionale, gli Stati membri dovrebbero incoraggiare i soggetti essenziali e importanti, in base alle norme applicabili ai procedimenti penali in conformità al diritto dell'Unione, a segnalare alle autorità di contrasto pertinenti gli incidenti di cui si sospetta la natura criminale grave. Ove opportuno, e fatte salve le norme in materia di protezione dei dati personali applicabili a Europol, è auspicabile che il Centro europeo per la lotta alla criminalità informatica (EC3) e l'ENISA agevolino il coordinamento tra le autorità competenti e le autorità di contrasto dei diversi Stati membri.

([21]) Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e che abroga la decisione (UE) 2015/2240 (GU L 166 dell'11.5.2021, pag. 1).

(108) In molti casi gli incidenti compromettono i dati personali. In tale contesto, 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.

(109) Il mantenimento di banche dati precise e complete dei dati di registrazione dei nomi di dominio («dati WHOIS») e la fornitura di un accesso legittimo a tali dati sono essenziali per garantire la sicurezza, la stabilità e la resilienza del DNS, che a sua volta contribuisce a un elevato livello comune di cibersicurezza in tutta l'Unione. A tal fine specifico, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a trattare alcuni dati necessari a raggiungere tale scopo. Tale trattamento dovrebbe costituire un obbligo legale ai sensi dell'articolo 6, paragrafo 1, lettera c), del regolamento (UE) 2016/679. Il suddetto obbligo non pregiudica la possibilità di raccogliere dati di registrazione dei nomi di dominio per altri scopi, ad esempio sulla base di accordi contrattuali o di obblighi legali stabiliti in altre normative dell'Unione o nazionali. Tale obbligo mira a ottenere una serie completa e accurata di dati di registrazione e non dovrebbe comportare la raccolta degli stessi dati più volte. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero cooperare tra loro al fine di evitare la duplicazione di tale compito.

(110) La disponibilità e la tempestiva accessibilità dei dati di registrazione dei nomi di dominio ai legittimi richiedenti l'accesso sono essenziali per la prevenzione e la lotta agli abusi del DNS, nonché per la prevenzione, l'individuazione e la risposta agli incidenti. Per legittimo richiedente l'accesso si intende qualsiasi persona fisica o giuridica che presenta una richiesta sulla base del diritto dell'Unione o nazionale. Possono comprendere autorità competenti a norma della presente direttiva e autorità competenti a norma del diritto dell'Unione o nazionale in materia di prevenzione, indagine, accertamento o perseguimento di reati, e CERT o CSIRT. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio, necessari ai fini della richiesta di accesso, ai legittimi richiedenti l'accesso, in conformità al diritto dell'Unione e nazionale. La richiesta dei legittimi richiedenti l'accesso dovrebbe essere corredata di una motivazione che consenta di valutare la necessità di accedere ai dati.

(111) Al fine di garantire la disponibilità di dati di registrazione dei nomi di dominio accurati e completi, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dovrebbero raccogliere i dati di registrazione dei nomi di dominio e garantirne l'integrità e la disponibilità. In particolare, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per raccogliere e mantenere i dati di registrazione dei nomi di dominio accurati e completi, nonché per prevenire e rettificare dati di registrazione inesatti in conformità al diritto dell'Unione in materia di protezione dei dati. Tali politiche e procedure dovrebbero tenere conto, nella misura del possibile, delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero adottare e attuare procedure proporzionate per verificare i dati di registrazione dei nomi di dominio. Tali procedure dovrebbero rispecchiare le migliori prassi utilizzate nel settore e, per quanto possibile, i progressi compiuti nel settore dell'identificazione elettronica. Tra gli esempi di procedure di verifica figurano i controlli ex ante effettuati al momento della registrazione e i controlli ex post effettuati dopo la registrazione. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero, in particolare, verificare almeno uno degli strumenti di contatto del soggetto che procede alla registrazione.

(112) I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a rendere pubblicamente disponibili i dati di registrazione dei nomi di dominio che non rientrano nell'ambito di applicazione delle norme dell'Unione in materia di protezione dei dati, come i dati riguardanti le persone giuridiche, in linea con il preambolo del regolamento (UE) 2016/679. Per le persone giuridiche, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero rendere pubblicamente disponibili almeno il nome del soggetto che procede alla registrazione e il numero di telefono di contatto. Anche l'indirizzo di posta elettronica di contatto dovrebbe essere pubblicato, a condizione che non contenga dati personali come alias di posta elettronica o account funzionali. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero inoltre consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio riguardanti le persone fisiche ai legittimi richiedenti l'accesso, in conformità al diritto dell'Unione in materia di protezione dei dati. Gli Stati membri dovrebbero imporre ai registri dei nomi di dominio di primo livello e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di rispondere senza indebito ritardo alle richieste di divulgazione dei dati di registrazione dei nomi di dominio presentate da legittimi richiedenti l'accesso.

I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per la pubblicazione e la divulgazione dei dati di registrazione, compresi accordi sul livello dei servizi, ai fini del trattamento delle richieste di accesso dei legittimi richiedenti l'accesso. Tali politiche e procedure dovrebbero tenere conto, nella misura del possibile, di eventuali orientamenti e delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. La procedura di accesso potrebbe comprendere l'uso di un'interfaccia, di un portale o di un altro strumento tecnico per fornire un sistema efficiente per la richiesta dei dati di registrazione e l'accesso agli stessi. Al fine di promuovere pratiche armonizzate in tutto il mercato interno, la Commissione può, fatte salve le competenze del comitato europeo per la protezione dei dati, fornire orientamenti su tali procedure che tengano conto, nella misura del possibile, delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. Gli Stati membri dovrebbero provvedere affinché tutte le modalità di accesso ai dati di registrazione dei nomi di dominio, a carattere personale e non, siano gratuite.

(113) I soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero essere considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti. Tuttavia, i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico dovrebbero essere considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi. I fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network dovrebbero essere considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. Gli enti della pubblica amministrazione dovrebbero rientrare nella giurisdizione dello Stato membro che li ha istituiti. Se fornisce servizi o è stabilito in più di uno Stato membro, il soggetto dovrebbe rientrare nella giurisdizione separata e concorrente di ciascuno di tali Stati membri. Le autorità competenti di tali Stati membri dovrebbero cooperare, prestarsi assistenza reciproca e, ove opportuno, condurre azioni comuni di vigilanza. Qualora esercitino la giurisdizione, gli Stati membri non dovrebbero imporre misure di esecuzione o comminare sanzioni più di una volta per lo stesso comportamento, in linea con il principio del ne bis in idem.

(114) Per tener conto della natura transfrontaliera dei servizi e delle attività dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei soggetti che forniscono servizi di registrazione dei nomi di dominio, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi gestiti, dei fornitori di servizi di sicurezza gestiti, nonché dei fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, tali soggetti dovrebbero essere posti sotto la giurisdizione di un solo Stato membro. La giurisdizione dovrebbe essere attribuita allo Stato membro in cui il soggetto interessato ha lo stabilimento principale nell'Unione. Il criterio dello stabilimento ai fini della presente direttiva implica l'esercizio effettivo dell'attività nel quadro di un'organizzazione stabile. A tale riguardo non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica. Il rispetto di tale criterio non dovrebbe dipendere dal fatto che i sistemi informatici e di rete siano situati fisicamente in un determinato luogo; la presenza e l'utilizzo dei sistemi in questione non costituiscono di per sé lo stabilimento principale e non sono pertanto criteri decisivi per la sua determinazione. Si dovrebbe considerare che lo stabilimento principale dovrebbe sia nello Stato membro in cui sono prevalentemente adottate nell'Unione le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Ciò corrisponderà di norma alla sede dell'amministrazione centrale dei soggetti nell'Unione. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui il soggetto ha lo stabilimento con il maggior numero di dipendenti nell'Unione. Qualora i servizi siano forniti da un gruppo di imprese, si dovrebbe considerare lo stabilimento principale dell'impresa controllante come lo stabilimento principale del gruppo di imprese.

(115) Quando un servizio DNS ricorsivo accessibile al pubblico è offerto da un fornitore di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico solo come parte del servizio di accesso a internet, il soggetto dovrebbe essere considerato sotto la giurisdizione di tutti gli Stati membri in cui i suoi servizi sono forniti.

(116) Qualora un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello, un soggetto che fornisce servizi di registrazione dei nomi di dominio, un fornitore di servizi di cloud computing, un fornitori di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti o un fornitore di un mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network non sia stabilito nell'Unione, ma offra servizi nell'Unione, esso dovrebbe designare un rappresentante nell'Unione. Per determinare se tale soggetto stia offrendo servizi nell'Unione, è opportuno verificare se il soggetto stia progettando di fornire servizi a persone in uno o più Stati membri. La semplice accessibilità nell'Unione del sito web del soggetto o di un intermediario, oppure di un indirizzo di posta elettronica o di altri dati di contatto, o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il soggetto è stabilito, dovrebbe essere considerata insufficiente per accertare tale intenzione. Tuttavia, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare servizi in tale lingua, o la menzione di clienti o utenti che si trovano nell'Unione, potrebbero evidenziare che il soggetto sta progettando di offrire servizi all'interno dell'Unione. Il rappresentante dovrebbe agire a nome del soggetto e le autorità competenti o i CSIRT dovrebbero poterlo contattare. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del soggetto affinché agisca a suo nome con riguardo agli obblighi di quest'ultimo ai sensi della presente direttiva, compresa la segnalazione di incidenti.

(117) Al fine di garantire una panoramica chiara dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei soggetti che forniscono servizi di registrazione dei nomi di dominio, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi gestiti, dei fornitori di servizi di sicurezza gestiti, nonché dei fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che offrono servizi nell'Unione rientranti nell'ambito di applicazione della presente direttiva, l'ENISA dovrebbe creare e mantenere un registro di tali entità, sulla base delle informazioni ricevute dagli Stati membri, se del caso attraverso i meccanismi nazionali istituiti per la loro registrazione. I punti di contatto unici dovrebbero trasmettere all'ENISA le informazioni ed eventuali modifiche apportate. Al fine di garantire l'accuratezza e la completezza delle informazioni che dovrebbero essere incluse in tale registro, gli Stati membri possono trasmettere all'ENISA le informazioni su tali soggetti disponibili in qualsiasi registro nazionale. L'ENISA e gli Stati membri dovrebbero adottare misure per agevolare l'interoperabilità di tali registri, garantendo nel contempo la protezione delle informazioni riservate o classificate. L'ENISA dovrebbe istituire adeguati protocolli di classificazione e gestione delle informazioni per garantire la sicurezza e la riservatezza delle informazioni divulgate e limitare l'accesso, l'archiviazione e la trasmissione di dette informazioni agli utenti destinatari.

(118) Qualora informazioni classificate in conformità al diritto nazionale o dell'Unione siano scambiate, comunicate o altrimenti condivise a norma della presente direttiva, dovrebbero essere applicate le corrispondenti norme sulla gestione delle informazioni classificate. Inoltre, l'ENISA dovrebbe predisporre l'infrastruttura, le procedure e le norme per il trattamento delle informazioni sensibili e classificate in conformità alle norme di sicurezza applicabili alla protezione delle informazioni classificate dell'UE.

(119) Di fronte a minacce informatiche che si fanno sempre più complesse e sofisticate, la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche che, a sua volta, accresce la capacità dei soggetti di impedire che tali minacce si trasformino in incidenti e consente ai soggetti di arginare in maniera più efficace gli effetti degli incidenti e di riprendersi in modo più efficiente. In assenza di orientamenti a livello dell'Unione, diversi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di concorrenza e responsabilità, sembrano aver ostacolato tale condivisione delle informazioni di intelligence.

(120) È quindi opportuno che i soggetti siano incoraggiati e assistiti dagli Stati membri al fine di sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le loro capacità di prevenire e rilevare adeguatamente gli incidenti, riprendersi da essi, rispondervi o mitigarne gli impatti. È pertanto necessario consentire la creazione a livello dell'Unione di accordi volontari di condivisione delle informazioni in materia di cibersicurezza. A tal fine, gli Stati membri dovrebbero sostenere e incoraggiare attivamente anche i soggetti quali i soggetti che forniscono servizi di cibersicurezza e di ricerca, nonché i soggetti pertinenti che non rientrano nell'ambito di applicazione della presente direttiva, a partecipare a tali accordi di condivisione delle informazioni in materia di cibersicurezza. Tali accordi dovrebbero essere stabiliti in conformità delle norme dell'Unione in materia di concorrenza e di protezione dei dati.

(121) Il trattamento dei dati personali, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete da parte di soggetti essenziali e importanti, potrebbe essere considerato lecito in virtù del fatto che tale trattamento è conforme a un obbligo legale cui è soggetto il titolare del trattamento, conformemente ai requisiti di cui all'articolo 6, paragrafo 1, lettera c), e all'articolo 6, paragrafo 3, del regolamento (UE) 2016/679. Il trattamento dei dati personali potrebbe essere necessario anche per i legittimi interessi perseguiti dai soggetti essenziali e importanti, nonché dai fornitori di tecnologie e servizi di sicurezza che agiscono per conto di tali soggetti, a norma dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679, anche qualora tale trattamento sia necessario per accordi di condivisione delle informazioni in materia di cibersicurezza o per la notifica volontaria di informazioni pertinenti a norma della presente direttiva. Le misure relative alla prevenzione, al rilevamento, all'individuazione, al contenimento e all'analisi degli incidenti e alla risposta agli stessi, le misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, lo scambio volontario di informazioni su tali incidenti, sulle minacce informatiche e sulle vulnerabilità, sugli indicatori di compromissione, sulle tattiche, sulle tecniche e le procedure, sugli allarmi di cibersicurezza e sugli strumenti di configurazione potrebbero richiedere il trattamento di talune categorie di dati personali, quali indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio, indirizzi di posta elettronica e, laddove rivelino dati personali, marcature temporali. Il trattamento dei dati personali da parte delle autorità competenti, dei punti di contatto unici e dei CSIRT potrebbe costituire un obbligo legale o essere considerato necessario per svolgere un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera c) o e), e dell'articolo 6, paragrafo 3, del regolamento (UE) 2016/679, o per perseguire un interesse legittimo dei soggetti essenziali e importanti di cui all'articolo 6, paragrafo 1, lettera f), di tale regolamento. Inoltre, il diritto nazionale potrebbe stabilire norme che consentano alle autorità competenti, ai punti di contatto unici e ai CSIRT, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti, di trattare categorie particolari di dati personali conformemente all'articolo 9 del regolamento (UE) 2016/679, in particolare prevedendo misure adeguate e specifiche per tutelare i diritti e gli interessi fondamentali delle persone fisiche, comprese limitazioni tecniche al riutilizzo di tali dati e l'uso di misure all'avanguardia in materia di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

(122) Al fine di rafforzare i poteri e le misure di vigilanza che contribuiscono a garantire l'effettiva conformità, la presente direttiva dovrebbe prevedere un elenco minimo di misure e mezzi di vigilanza attraverso i quali le autorità competenti possono vigilare sui soggetti essenziali e importanti. La presente direttiva dovrebbe inoltre stabilire una differenziazione del regime di vigilanza tra i soggetti essenziali e i soggetti importanti al fine di garantire un giusto equilibrio degli obblighi per tali soggetti e per le autorità competenti. Pertanto, i soggetti essenziali dovrebbero essere sottoposti a un regime di vigilanza completo, ex ante ed ex post, mentre i soggetti importanti dovrebbero essere sottoposti a un regime di vigilanza leggero, solo ex post. I soggetti importanti non dovrebbero quindi essere tenuti a documentare sistematicamente il rispetto delle misure di gestione dei rischi di cibersicurezza, mentre le autorità competenti dovrebbero attuare un approccio ex post reattivo alla vigilanza e, di conseguenza, non dovrebbero avere un obbligo generale di vigilanza su tali soggetti. La vigilanza ex post di soggetti importanti può essere innescata da elementi di prova, indicazioni o informazioni portati all'attenzione delle autorità competenti che tali autorità ritengono suggerire possibili violazioni della presente direttiva. Ad esempio, tali elementi di prova, indicazioni o informazioni potrebbero essere del tipo fornito alle autorità competenti da altre autorità, soggetti, cittadini, media o altre fonti o informazioni disponibili al pubblico, o emergere nel corso di altre attività svolte dalle autorità competenti nell'adempimento dei loro compiti.

(123) L'esecuzione dei compiti di vigilanza da parte delle autorità competenti non dovrebbe ostacolare inutilmente le attività commerciali del soggetto interessato. Nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, tra cui lo svolgimento di ispezioni in loco e la vigilanza a distanza, le indagini sui casi di violazione della presente direttiva e lo svolgimento di audit sulla sicurezza o scansioni di sicurezza, le autorità competenti dovrebbero ridurre al minimo l'impatto sulle attività commerciali del soggetto interessato.

(124) Nell'esercizio della vigilanza ex ante, le autorità competenti dovrebbero poter decidere in modo proporzionato l'ordine di priorità nel ricorso alle misure e ai mezzi di vigilanza a loro disposizione. Ciò implica che le autorità competenti possano decidere l'ordine di priorità sulla base di metodologie di vigilanza che dovrebbero seguire un approccio basato sui rischi. Più specificamente, tali metodologie potrebbero includere criteri o parametri di riferimento per la classificazione dei soggetti essenziali in categorie di rischio e corrispondenti misure e mezzi di vigilanza raccomandati per categoria di rischio, quali l'uso, la frequenza o il tipo di ispezioni in loco, audit sulla sicurezza mirati o scansioni di sicurezza, il tipo di informazioni da richiedere e il livello di dettaglio di tali

informazioni. Tali metodologie di vigilanza potrebbero inoltre essere corredate da programmi di lavoro ed essere valutate e riesaminate periodicamente, anche per quanto riguarda aspetti quali l'assegnazione e il fabbisogno di risorse. In relazione agli enti della pubblica amministrazione, i poteri di vigilanza dovrebbero essere esercitati in linea con i quadri legislativi e istituzionali nazionali.

(125) Le autorità competenti dovrebbero provvedere affinché i loro compiti di vigilanza nei confronti dei soggetti essenziali e importanti siano svolti da professionisti formati, che dovrebbero disporre delle competenze necessarie per svolgere tali compiti, in particolare per quanto riguarda lo svolgimento di ispezioni in loco e la vigilanza a distanza, compresa l'individuazione di carenze nelle banche dati, nell'hardware, nei firewall, nella cifratura e nelle reti. Tali ispezioni e tale supervisione dovrebbero essere condotte in modo obiettivo.

(126) In casi debitamente giustificati in cui sia a conoscenza di una minaccia informatica significativa o di un rischio imminente, l'autorità competente dovrebbe essere in grado di adottare decisioni di esecuzione immediata al fine di prevenire un incidente o di rispondervi.

(127) Al fine di rendere efficace l'esecuzione, è opportuno stabilire un elenco minimo di competenze di esecuzione che possono essere esercitate in caso di violazione delle misure di gestione e segnalazione dei rischi di cibersicurezza previsti dalla presente direttiva, istituendo un quadro chiaro e coerente per tali misure di esecuzione in tutta l'Unione. Occorre tenere debitamente conto della natura, della gravità e della durata del danno materiale o immateriale causato, del carattere doloso o colposo della violazione della presente direttiva, delle azioni intraprese per prevenire o attenuare il danno materiale o immateriale, del grado di responsabilità o di eventuali violazioni precedenti pertinenti, del grado di cooperazione con l'autorità competente e di qualsiasi altro fattore aggravante o attenuante. Le misure di esecuzione, comprese le sanzioni amministrative pecuniarie, dovrebbero essere proporzionate e la loro imposizione dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea («Carta»), inclusi il diritto a un ricorso effettivo e a un giusto processo, la presunzione di innocenza e i diritti della difesa.

(128) La presente direttiva non impone agli Stati membri di prevedere la responsabilità penale o civile delle persone fisiche incaricate di garantire la conformità di un soggetto alla presente direttiva per i danni subiti da terzi a seguito di una violazione della stessa.

(129) Al fine di garantire l'efficace applicazione degli obblighi stabiliti nella presente direttiva, ciascuna autorità competente dovrebbe avere il potere di imporre o chiedere l'imposizione di sanzioni amministrative pecuniarie.

(130) Qualora una sanzione amministrativa pecuniaria sia comminata a un soggetto essenziale o importante che è un'impresa, quest'ultima dovrebbe essere intesa quale impresa conformemente agli articoli 101 e 102 TFUE a tali fini. Qualora una sanzione amministrativa pecuniaria sia comminata a una persona che non sia impresa, l'autorità competente dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. L'imposizione di una sanzione amministrativa pecuniaria non pregiudica l'applicazione di altri poteri da parte delle autorità competenti o di altre sanzioni previste dalle norme nazionali di recepimento della presente direttiva.

(131) Gli Stati membri dovrebbero poter stabilire le norme relative alle sanzioni penali in caso di violazione delle norme nazionali di recepimento della presente direttiva. Tuttavia, l'imposizione di sanzioni penali per le violazioni di tali norme nazionali e delle relative sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia dell'Unione europea.

(132) Qualora la presente direttiva non armonizzi le sanzioni amministrative o ove necessario in altri casi, ad esempio in caso di violazione grave degli obblighi della presente direttiva, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, e se esse siano penali o amministrative, dovrebbe essere determinata dalla legislazione nazionale.

(133) Al fine di rafforzare ulteriormente l'efficacia e il carattere dissuasivo delle misure di esecuzione applicabili alle violazioni della presente direttiva, le autorità competenti dovrebbero avere la facoltà di sospendere temporaneamente o di richiedere la sospensione temporanea di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi pertinenti forniti o dalle attività effettuate da un soggetto essenziale e richiedere l'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di qualsiasi persona fisica che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale. Data la loro gravità e l'impatto sulle attività dei soggetti e, in ultima analisi, sugli utenti, tali sospensioni o divieti temporanei dovrebbero essere applicati solo in proporzione alla gravità della violazione e tenendo conto delle circostanze di ciascun singolo caso, tra cui il carattere doloso o colposo della violazione e qualsiasi azione intrapresa per prevenire o attenuare il danno materiale o immateriale Tali sospensioni o divieti temporanei dovrebbero essere applicati solo come ultima ratio, vale a dire solo una volta esaurite le altre pertinenti misure di esecuzione previste dalla presente direttiva, e solo fino a quando il soggetto interessato non adotti le misure necessarie per rimediare alle carenze o per conformarsi alle prescrizioni dell'autorità competente per cui tali sospensioni o divieti temporanei sono stati applicati. L'imposizione di tali sospensioni o i divieti temporanei dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad un giusto processo, la presunzione di innocenza e i diritti della difesa.

(134) Al fine di garantire l'adempimento, da parte dei soggetti, degli obblighi di cui alla presente direttiva, gli Stati membri dovrebbero cooperare e prestarsi reciproca assistenza per quanto riguarda le misure di vigilanza e di applicazione, in particolare quando un soggetto fornisce servizi in più di uno Stato membro o quando i suoi sistemi informatici e di rete sono situati in uno Stato membro diverso da quello in cui presta servizi. Nel fornire assistenza, l'autorità competente interpellata dovrebbe adottare misure di vigilanza o di esecuzione conformemente al diritto nazionale. Onde garantire il buon funzionamento dell'assistenza reciproca ai sensi della presente direttiva, le autorità competenti dovrebbero avvalersi del gruppo di cooperazione quale forum per esaminare i singoli casi e le richieste di assistenza.

(135) Al fine di garantire una vigilanza e un'esecuzione efficaci, in particolare quando la situazione ha una dimensione transfrontaliera, gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca dovrebbero, nei limiti di tale richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto oggetto di tale richiesta, e che fornisce servizi o che dispone di sistemi informatici e di una rete sul territorio di tale Stato membro.

(136) La presente direttiva dovrebbe stabilire norme di cooperazione tra le autorità competenti e le autorità di controllo nel quadro del regolamento (UE) 2016/679 per far fronte alle violazioni della presente direttiva relative ai dati personali.

(137) La presente direttiva dovrebbe mirare a garantire un elevato livello di responsabilità per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a livello di soggetti essenziali e importanti. Pertanto, gli organi di gestione dei soggetti essenziali e importanti dovrebbero approvare le misure di gestione dei rischi di cibersicurezza e sorvegliarne l'attuazione.

(138) Al fine di garantire un livello comune elevato di cibersicurezza in tutta l'Unione sulla base della presente direttiva, conformemente all'articolo 290 TFUE alla Commissione dovrebbe essere delegato il potere di adottare atti per quanto riguarda l'integrazione della presente direttiva specificando quali categorie di soggetti essenziali e importanti debbano essere tenute ad utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o ad ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([22]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

([22]) GU L 123 del 12.5.2016, pag. 1.

(139) Al fine di garantire condizioni uniformi per l'attuazione della presente direttiva, dovrebbero essere attribuite alla Commissione competenze di esecuzione per stabilire le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione e i requisiti tecnici e metodologici nonché settoriali relativi alle misure di gestione del rischio di cibersicurezza, e per specificare ulteriormente il tipo di informazioni, il formato e la procedura degli incidenti, delle minacce informatiche e delle notifiche quasi assenti e delle comunicazioni significative relative a minacce informatiche, nonché i casi in cui un incidente deve essere considerato significativo. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([23]).

(140) È opportuno che la Commissione riesamini la presente direttiva a scadenze regolari, dopo aver consultato le parti interessate, in particolare al fine valutare se sia opportuno proporre modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato. Nel quadro di tali riesami, la Commissione dovrebbe valutare la pertinenza delle dimensioni dei soggetti interessati, e i settori, dei sottosettori e dei tipi di soggetto di cui agli allegati della presente direttiva ai fini del funzionamento dell'economia e della società per quanto riguarda la cibersicurezza. La Commissione dovrebbe valutare, tra l'altro, se i fornitori, che ricadono nell'ambito di applicazione della presente direttiva, designati come piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio ([24]) possano essere identificati come soggetti essenziali ai sensi della presente direttiva.

(141) La presente direttiva istituisce nuovi compiti per l'ENISA, rafforzando in tal modo il suo ruolo, e potrebbe anche portare l'ENISA a dover svolgere i suoi compiti a norma del regolamento (UE) 2019/881 a un livello più alto di prima. Al fine di garantire che l'ENISA disponga delle risorse finanziarie e umane necessarie per svolgere le funzioni esistenti e nuove, nonché per soddisfare eventuali livelli più elevati di esecuzione di tali funzioni derivanti dal suo ruolo rafforzato, il suo bilancio dovrebbe essere aumentato di conseguenza. Inoltre, al fine di garantire un uso efficiente delle risorse, all'ENISA dovrebbe essere data maggiore flessibilità nel modo in cui è in grado di assegnare risorse internamente, in modo che possa svolgere i suoi compiti e soddisfare le aspettative in modo efficace.

(142) Poiché l'obiettivo della presente direttiva, vale a dire conseguire un elevato livello comune di cibersicurezza nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(143) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà d'impresa, il diritto alla proprietà, il diritto a un ricorso effettivo e ad un giudice imparziale, la presunzione d'innocenza e i diritti della difesa. Il diritto a un ricorso effettivo si estende ai destinatari di servizi forniti da soggetti essenziali e importanti. La presente direttiva dovrebbe essere attuata in conformità a tali diritti e principi.

(144) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([25]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere l'11 marzo 2021 ([26]),

---

([23]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([24]) Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

([25]) 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).

([26]) GU C 183 dell'11.5.2021, pag. 3.

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno.

2. A tal fine, la presente direttiva stabilisce:

a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);

b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;

c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza;

d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione.

L'articolo 3, paragrafo 4, dell'allegato a tale raccomandazione non si applica ai fini della presente direttiva.

2. La presente direttiva si applica anche ai soggetti, indipendentemente dalle loro dimensioni, delle tipologie di cui all'allegato I o II qualora:

a) i servizi siano forniti da:

   i) fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;

   ii) prestatore di servizi di fiducia;

   iii) registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;

b) il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;

c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

f) il soggetto è un ente della pubblica amministrazione:

i) dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale; o

ii) a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche.

3. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557.

4. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, che forniscono servizi di registrazione dei nomi di dominio.

5. Gli Stati membri possono prevedere che la presente direttiva si applichi a:

a) enti della pubblica amministrazione a livello locale;

b) istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.

6. La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

7. La presente direttiva non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

8. Gli Stati membri possono esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o del contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui al paragrafo 7 del presente articolo, dal rispetto degli obblighi di cui all'articolo 21 o all'articolo 23 per quanto riguarda tali attività o servizi. In tali casi, le misure di vigilanza e di applicazione di cui al capo VII non si applicano in relazione a tali attività o servizi specifici. Qualora i soggetti svolgano attività o prestino servizi esclusivamente del tipo di cui al presente paragrafo, gli Stati membri possono anche decidere di esentare tali enti dagli obblighi di cui agli articoli 3 e 27.

9. I paragrafi 7 e 8 non si applicano quando un soggetto agisce in qualità di prestatore di servizi fiduciari.

10. La presente direttiva non si applica ai soggetti che gli Stati membri hanno esentato dall'ambito di applicazione del regolamento (UE) 2022/2554 ai sensi dell'articolo 2, paragrafo 4, di tale regolamento.

11. Gli obblighi stabiliti nella presente direttiva non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

12. La presente direttiva si applica fatti salvi il regolamento (UE) 2016/679, la direttiva 2002/58/CE, le direttive 2011/93/UE ([27]) e 2013/40/UE ([28]) del Parlamento europeo e del Consiglio e la direttiva (UE) 2022/2557.

13. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione o nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti conformemente alla presente direttiva solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali di soggetti interessati.

([27]) Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

([28]) Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

14. I soggetti, le autorità competenti, i punti di contatto unici e i CSIRT trattano i dati personali nella misura necessaria ai fini della presente direttiva e conformemente al regolamento (UE) 2016/679, in particolare tale trattamento si basa sull'articolo 6 dello stesso.

Il trattamento dei dati personali a norma della presente direttiva da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di comunicazioni elettroniche accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione in materia di protezione dei dati e della legislazione dell'Unione in materia di riservatezza, segnatamente la direttiva 2002/58/CE.

Articolo 3

Soggetti essenziali e importanti

1. Ai fini della presente direttiva, sono considerati soggetti essenziali i seguenti:

a) soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;

c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla raccomandazione 2003/361/CE;

d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i);

e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

f) soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557, di cui all'articolo 2, paragrafo 3 della presente direttiva;

g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale.

2. Ai fini della presente direttiva, sono considerati soggetti importanti i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del paragrafo 1 del presente articolo. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

3. Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Successivamente, gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

4. Ai fini della compilazione dell'elenco di cui al paragrafo 3, gli Stati membri impongono alle entità di cui a tale paragrafo di presentare alle autorità competenti almeno le informazioni seguenti:

a) il proprio nome;

b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail, le serie di IP e i numeri di telefono;

c) se del caso, i settori e sottosettori pertinenti di cui all'allegato I o II; e

d) se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della presente direttiva.

I soggetti di cui al paragrafo 3 notificano tempestivamente qualsiasi modifica delle informazioni trasmesse a norma del primo comma del presente paragrafo e in ogni caso entro due settimane dalla data della modifica.

La Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornisce senza indebito ritardo orientamenti e modelli relativi agli obblighi di cui al presente paragrafo.

Gli Stati membri possono istituire meccanismi nazionali che consentano alle entità di registrarsi.

5. Entro il 17 aprile 2025 e successivamente ogni due anni, le autorità competenti notificano:

a) alla Commissione e al gruppo di coordinamento, il numero dei soggetti essenziali e importanti elencati ai sensi del paragrafo 3 per ciascun settore e sottosettore di cui all'allegato I o II; e

b) alla Commissione informazioni pertinenti sul numero di soggetti essenziali e importanti individuati ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e), sul settore e il sottosettore di cui all'allegato I o II cui appartengono, sul tipo di servizio che forniscono e sulla fornitura, tra quelli stabiliti all'articolo 2, paragrafo 2, lettere da b) a e), ai sensi dei quali sono stati individuati.

6. Sino al 17 aprile 2025 e su richiesta della Commissione, gli Stati membri possono notificare alla Commissione i nomi dei soggetti essenziali e importanti di cui al paragrafo 5, lettera b).

Articolo 4

Atti giuridici settoriali dell'Unione

1. Qualora gli atti giuridici settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti significativi, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, a tali soggetti non si applicano le pertinenti disposizioni della presente direttiva, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VII. Qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva continuano ad applicarsi ai soggetti non contemplati da tali atti giuridici settoriali dell'Unione.

2. I requisiti di cui al paragrafo 1 del presente articolo sono considerati di effetto equivalente agli obblighi stabiliti dalla presente direttiva qualora:

a) gli effetti delle misure di gestione dei rischi di cibersicurezza siano almeno equivalenti a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2; oppure

b) l'atto giuridico settoriale dell'Unione preveda l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte dei CSIRT, delle autorità competenti o dei punti di contatto unici a norma della presente direttiva e qualora gli obblighi di notifica degli incidenti significativi abbiano un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della presente direttiva.

3. La Commissione, entro il 17 luglio 2023, fornisce orientamenti che chiariscano l'applicazione dei paragrafi 1 e 2. La Commissione rivede tali orientamenti periodicamente. Nella preparazione di detti orientamenti, la Commissione tiene conto delle osservazioni del gruppo di cooperazione e dell'ENISA.

Articolo 5

Armonizzazione minima

La presente direttiva non impedisce agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.

Articolo 6

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) «sistema informatico e di rete»:

   a) una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972;

b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o

c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

2) «sicurezza dei sistemi informatici e di rete»: la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi;

3) «cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881;

4) «strategia nazionale per la cibersicurezza»: un quadro coerente di uno Stato membro che prevede priorità e obiettivi strategici in materia di cibersicurezza e la governance per il loro conseguimento in tale Stato membro;

5) «quasi incidente»: un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato;

6) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;

7) «incidente di cibersicurezza su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

8) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso;

9) «rischio»: la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi;

10) «minaccia informatica»: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

11) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi del soggetto causando perdite materiali o immateriali considerevoli;

12) «prodotto TIC»: un prodotto TIC quale definito all'articolo 2, punto 12), del regolamento (UE) 2019/881;

13) «servizio TIC»: un servizio TIC quale definito all'articolo 2, punto 13), del regolamento (UE) 2019/881;

14) «processo TIC»: un processo TIC quale definito all'articolo 2, punto 14), del regolamento (UE) 2019/881;

15) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

16) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([29]);

17) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012;

([29]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

18) «punto di interscambio internet»: un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico;

19) «sistema dei nomi di dominio» o «DNS»: un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di inoltro e connettività di internet al fine di accedere a tali servizi e risorse;

20) «fornitore di servizi DNS»: un soggetto che fornisce:

a) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet; o

b) servizi di risoluzione dei nomi di dominio autorevoli per uso da parte di terzi, fatta eccezione per i server dei nomi radice;

21) «registro dei nomi di dominio di primo livello» o «registro dei nomi TLD»: un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situazioni in cui i nomi TLD sono utilizzati da un registro esclusivamente per uso proprio;

22) «soggetto che fornisce servizi di registrazione di nomi di dominio»: un registrar o un agente che agisce per conto di registrar, come un fornitore o un rivenditore di servizi di registrazione per la privacy o di proxy;

23) «servizio digitale»: un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([30]);

24) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014;

25) «prestatore di servizi fiduciari»: un prestatore di servizi fiduciari quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014;

26) «servizio fiduciario qualificato»: un servizio fiduciario qualificato quale definito all'articolo 3, punto 17), del regolamento (UE) n. 910/2014;

27) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari qualificato quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014;

28) «mercato online»: un mercato online quale definito all'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio ([31]);

29) «motore di ricerca online»: un motore di ricerca online quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio ([32]);

30) «servizio di cloud computing»: un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni.

([30]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([31]) Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») (GU L 149 dell'11.6.2005, pag. 22).

([32]) Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (GU L 186 dell'11.7.2019, pag. 57).

31) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

32) «rete di distribuzione dei contenuti (*content delivery network*)»: una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di internet per conto di fornitori di contenuti e servizi;

33) «piattaforma di servizi di social network»: una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi, in particolare, attraverso chat, post, video e raccomandazioni;

34) «rappresentante»: una persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di cloud computing, un fornitore di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva;

35) «ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, che non comprende la magistratura, i parlamenti e le banche centrali, che soddisfa i criteri seguenti:

    a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

    b) è dotato di personalità giuridica o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica;

    c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;

    d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali;

36) «rete pubblica di comunicazione elettronica»: una rete pubblica di comunicazione elettronica quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972;

37) «servizio di comunicazione elettronica»: un servizio di comunicazione elettronica quale definito all'articolo 2, punto 4), della direttiva (UE) 2018/1972;

38) «soggetto»: una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

39) «fornitore di servizi gestiti»: un soggetto che fornisce servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informatico e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza;

40) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi di sicurezza gestiti che svolge o fornisce assistenza per attività relative alla gestione dei rischi di cibersicurezza;

41) «organismo di ricerca»: un soggetto che ha come obiettivo principale lo svolgimento di attività di ricerca applicata o di sviluppo sperimentale al fine di sfruttare i risultati di tale ricerca a fini commerciali, ma che non comprende gli istituti di istruzione.

CAPO II

QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA

Articolo 7

Strategia nazionale per la cibersicurezza

1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che prevede gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza. La strategia nazionale per la cibersicurezza comprende:

a) gli obiettivi e le priorità della strategia per la cibersicurezza dello Stato membro, che riguardano in particolare i settori di cui agli allegati I e II;

b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera a) del presente paragrafo, comprendente le misure strategiche di cui al paragrafo 2;

c) un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le autorità competenti, i punti di contatto unici e i CSIRT ai sensi della presente direttiva, nonché il coordinamento e la cooperazione tra tali organismi e le autorità competenti ai sensi degli atti giuridici settoriali dell'Unione;

d) un meccanismo per individuare le risorse e una valutazione dei rischi nello Stato membro in questione;

e) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;

f) un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cibersicurezza;

g) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e le autorità competenti a norma della direttiva (UE) 2022/2557 ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, se del caso;

h) un piano, comprendente le misure necessarie, per aumentare livello generale di consapevolezza dei cittadini in materia di cibersicurezza.

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare misure strategiche riguardanti:

a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi;

b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source;

c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1;

d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del carattere fondamentale pubblico di una rete internet aperta, compresa, se del caso, la cibersicurezza dei cavi di comunicazione sottomarini;

e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate pertinenti miranti ad attuare misure di avanguardia nella gestione dei rischi di cibersicurezza;

f) la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di cibersicurezza, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti;

g) il sostegno agli istituti accademici e di ricerca volto a sviluppare, rafforzare e promuovere la diffusione di strumenti di cibersicurezza e di infrastrutture di rete sicure;

h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra soggetti, nel rispetto del diritto dell'Unione;

i) il rafforzamento dei valori di riferimento relativi alla ciberresilienza e all'igiene informatica delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche;

j) la promozione di una protezione informatica attiva.

3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. Gli Stati membri possono omettere dalla notifica informazioni relative alla propria sicurezza nazionale.

4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni cinque anni sulla base di indicatori chiave di prestazione e, se necessario, le aggiornano. L'ENISA assiste gli Stati membri, su richiesta di questi ultimi, nell'elaborazione o aggiornamento di una strategia nazionale per la cibersicurezza e di indicatori chiave di prestazione per la relativa valutazione, onde allinearla ai requisiti e agli obblighi di cui alla presente direttiva.

Articolo 8

Autorità competenti e punti di contatto unici

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VII (autorità competenti).

2. Le autorità competenti di cui al paragrafo 1 controllano l'attuazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa o istituisce un punto di contatto unico. Se uno Stato membro designa o istituisce soltanto un'autorità competente a norma del paragrafo 1, quest'ultima è anche il punto di contatto unico per tale Stato membro.

4. Ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro.

5. Gli Stati membri garantiscono che le proprie autorità competenti e i propri punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva.

6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'identità dell'autorità competente di cui al paragrafo 1 e del punto di contatto unico di cui al paragrafo 3, i compiti di tali autorità e qualsiasi ulteriore modifica dei medesimi. Ciascuno Stato membro rende pubblica l'identità della propria autorità competente. La Commissione elabora un elenco dei punti di contatto unici disponibili.

Articolo 9

Quadri nazionali di gestione delle crisi informatiche

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala (autorità di gestione delle crisi informatiche). Gli Stati membri provvedono affinché tali autorità dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente. Gli Stati membri assicurano la coerenza con i quadri nazionali esistenti di gestione generale delle crisi.

2. Se uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala.

3. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva.

4. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala in cui sono stabiliti gli obiettivi e le modalità della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. In tale piano sono definiti, in particolare:

a) gli obiettivi delle misure e delle attività nazionali di preparazione;

b) i compiti e le responsabilità delle autorità di gestione delle crisi informatiche;

c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi e i canali di scambio di informazioni;

d) le misure nazionali di preparazione, comprese le esercitazioni e le attività di formazione;

e) i pertinenti portatori di interessi del settore pubblico e privato e le infrastrutture coinvolte;

f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dello Stato membro alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello dell'Unione.

5. Entro tre mesi dalla designazione o istituzione dell'autorità di gestione delle crisi informatiche di cui al paragrafo 1, ciascuno Stato membro notifica alla Commissione l'identità della propria autorità e qualsiasi ulteriore modifica alla stessa. Gli Stati membri presentano alla Commissione e alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui al paragrafo 4 in merito ai propri piani nazionali di risposta agli incidenti e delle crisi di cibersicurezza su vasta scala entro tre mesi dall'adozione di tali piani. Gli Stati membri possono omettere informazioni se e nella misura in cui ciò sia necessario ai fini della loro sicurezza nazionale.

Articolo 10

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

1. Ogni Stato membro designa o istituisce uno o più CSIRT. È possibile designare o istituire i CSIRT all'interno di un'autorità competente. I CSIRT sono conformi ai requisiti di cui all'articolo 11, paragrafo 1, si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita.

2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 11, paragrafo 3.

3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. A tal fine gli Stati membri provvedono affinché ogni CSIRT contribuisca allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 29 con comunità settoriali o intersettoriali di soggetti essenziali e importanti.

5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 19.

6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT.

7. I CSIRT possono stabilire relazioni di cooperazione con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi. Nell'ambito di tali relazioni di cooperazione, gli Stati membri facilitano uno scambio di informazioni efficace, efficiente e sicuro con tali team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP (*Traffic Light Protocol*). I CSIRT possono scambiare informazioni pertinenti con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, compresi dati personali a norma del diritto dell'Unione in materia di protezione dei dati.

8. I CSIRT possono cooperare con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi o con organismi equivalenti di paesi terzi, in particolare al fine di fornire loro assistenza in materia di cibersicurezza.

9. Ogni Stato membro notifica alla Commissione senza indebiti ritardi l'identità del CSIRT di cui al paragrafo 1 del presente articolo e del CSIRT designato come coordinatore conformemente all'articolo 12, paragrafo 1, i rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi.

10. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo dei CSIRT.

Articolo 11

Requisiti, capacità tecniche e compiti dei CSIRT

1. I CSIRT soddisfano i requisiti seguenti:

a) i CSIRT garantiscono un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di vulnerabilità (*single points of failure*) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento; essi indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;

b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;

c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

d) i CSIRT garantiscono la riservatezza e l'affidabilità delle loro operazioni;

e) i CSIRT dispongono di personale sufficiente per garantire la disponibilità dei loro servizi in qualsiasi momento e garantiscono che il loro personale sia formato in modo appropriato;

f) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi.

I CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.

2. Gli Stati membri assicurano che i loro CSIRT dispongano congiuntamente delle capacità tecniche necessarie a svolgere i compiti di cui al paragrafo 3. Gli Stati membri provvedono affinché ai propri CSIRT siano assegnate risorse sufficienti per garantire un organico adeguato al fine di consentire ai CSIRT di sviluppare le proprie capacità tecniche.

3. I CSIRT svolgono i compiti seguenti:

a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete;

b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;

c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso;

d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;

e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;

f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta.

g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1;

h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui all'articolo 10, paragrafo 3.

I CSIRT possono effettuare una scansione proattiva e non intrusiva dei sistemi informatici e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informatici e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.

Nello svolgimento dei compiti di cui al primo comma, i CSIRT possono dare priorità a determinati compiti sulla base di un approccio basato sul rischio.

4. I CSIRT instaurano rapporti di cooperazione con i pertinenti portatori di interesse del settore privato al fine di perseguire gli obiettivi della presente direttiva.

5. Al fine di agevolare la cooperazione di cui al paragrafo 4, i CSIRT promuovono l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la gestione delle crisi; e

c) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1.

Articolo 12

Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità

1. Ogni Stato membro designa uno dei propri CSIRT come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti. I compiti del CSIRT designato come coordinatore comprendono:

a) l'individuazione e il contatto dei soggetti interessati;

b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, e

c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.

Gli Stati membri provvedono affinché le persone fisiche o giuridiche possano segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT designato come coordinatore. Il CSIRT designato come coordinatore garantisce lo svolgimento di diligenti azioni per dare seguito alla segnalazione di vulnerabilità e assicura l'anonimato della persona fisica o giuridica segnalante. Se la vulnerabilità segnalata è suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro, il CSIRT designato di ciascuno Stato membro interessato coopera, se del caso, con altri CSIRT designati in qualità di coordinatori nell'ambito della rete di CSIRT.

2. L'ENISA elabora e mantiene, previa consultazione del gruppo di cooperazione, una banca dati europea delle vulnerabilità. A tal fine l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati e adotta le necessarie misure tecniche e organizzative per garantire la sicurezza e l'integrità della banca dati europea delle vulnerabilità, in particolare al fine di consentire ai soggetti, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, e ai relativi fornitori di sistemi informatici e di rete, di divulgare e registrare, su base volontaria, le vulnerabilità pubblicamente note presenti nei prodotti TIC o nei servizi TIC. Tutti i portatori di interessi hanno accesso alle informazioni sulle vulnerabilità contenute nella banca dati europea delle vulnerabilità. La banca dati contiene:

a) informazioni che illustrano la vulnerabilità;

b) i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata;

c) la disponibilità di relative patch e, qualora queste non fossero disponibili, gli orientamenti forniti dalle autorità nazionali competenti o dai CSIRT rivolti agli utenti dei prodotti TIC e dei servizi TIC vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate.

Articolo 13

Cooperazione a livello nazionale

1. Se sono separati, le autorità competenti, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva.

2. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti, ricevano le notifiche degli incidenti significativi a norma dell'articolo 23, nonché degli incidenti, delle minacce informatiche e dei quasi incidenti (*near miss*) a norma dell'articolo 30.

3. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti informino i loro punti di contatto unico delle notifiche relative agli incidenti, alle minacce informatiche e ai quasi incidenti trasmesse a norma della presente direttiva.

4. Al fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione.

5. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma della direttiva (UE) 2022/2557 collaborino e si scambino periodicamente informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti essenziali identificati come critici a norma della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti. Gli Stati membri provvedono inoltre affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma del regolamento (UE) n. 910/2014, del regolamento (UE) 2022/2554 e della direttiva (UE) 2018/1972 si scambino periodicamente informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

6. Gli Stati membri semplificano la comunicazione mediante i mezzi tecnici per le notifiche di cui agli articoli 23 e 30.

CAPO III

COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE

Articolo 14

Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri, nonché di rafforzare la fiducia, è istituito un gruppo di cooperazione.

2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 7.

3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il Servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) e le autorità competenti a norma del regolamento (UE) 2022/2554 possono partecipare alle attività del gruppo di cooperazione conformemente all'articolo 47, paragrafo 1, di tale regolamento.

Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori il Parlamento europeo e i rappresentanti dei pertinenti portatori di interessi.

La Commissione ne assicura il segretariato.

4. Il gruppo di cooperazione svolge i compiti seguenti:

a) fornire orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva;

b) fornire orientamenti alle autorità competenti in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 7, paragrafo 2, lettera c);

c) scambiare migliori prassi e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche, nonché l'identificazione dei soggetti essenziali e importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

d) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza e la coerenza globale dei requisiti settoriali di cibersicurezza;

e) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda i progetti di atti delegati o di esecuzione adottati a norma della presente direttiva;

f) scambiare migliori prassi e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione;

g) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione che contengono disposizioni in materia di cibersicurezza;

h) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9 ed elaborare conclusioni e raccomandazioni;

i) effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1;

j) discutere i casi di assistenza reciproca, fra cui le esperienze e i risultati delle azioni di vigilanza comuni transfrontaliere di cui all'articolo 37;

k) su richiesta di uno o più Stati membri interessati, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 37;

l) fornire orientamenti strategici alla rete di CSIRT ed EU–CyCLONe su specifiche questioni emergenti;

m) effettuare scambi di opinioni sulla politica in materia di azioni di follow-up a seguito incidenti e crisi di cibersicurezza su vasta scala sulla base degli insegnamenti tratti dalla rete di CSIRT e da EU-CyCLONe;

n) contribuire alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolga il personale delle autorità competenti o dei CSIRT;

o) organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere contributi sulle sfide strategiche emergenti;

p) discutere le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA;

q) stabilire la metodologia e gli aspetti organizzativi delle revisioni tra pari di cui all'articolo 19, paragrafo 1, nonché stabilire, con l'assistenza della Commissione e dell'ENISA, la metodologia di autovalutazione per gli Stati membri a norma dell'articolo 19, paragrafo 4, ed elaborare, in collaborazione con la Commissione e l'ENISA, i codici di condotta su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati a norma dell'articolo 19, paragrafo 6;

r) elaborare relazioni, ai fini del riesame di cui all'articolo 40, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari;

s) discutere e svolgere periodicamente una valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware.

Il gruppo di cooperazione presenta le relazioni di cui al primo comma, lettera r), alla Commissione, al Parlamento europeo e al Consiglio.

5. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro rappresentanti in seno al gruppo di cooperazione.

6. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.

7. Entro il 1º febbraio 2024 e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti.

8. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo comma del presente paragrafo, conformemente al paragrafo 4, lettera e).

9. Il gruppo di cooperazione si riunisce periodicamente, e in ogni caso una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) 2022/2557 al fine di promuovere e agevolare la cooperazione strategica e lo scambio di informazioni.

Articolo 15

Rete di CSIRT

1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

2. La rete di CSIRT è composta da rappresentanti dei CSIRT designati o istituiti a norma dell'articolo 10 e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE). La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT.

3. La rete di CSIRT svolge i compiti seguenti:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;

b) agevolare la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT;

c) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità;

d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza;

e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;

f) su richiesta di un membro della rete di CSIRT potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati;

g) su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;

i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

j) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

   i) categorie di minacce informatiche e incidenti;

   ii) preallarmi;

   iii) assistenza reciproca;

   iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

   v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro;

k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito;

l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA;

m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9;

p) fornire orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

4. Entro il 17 gennaio 2025, e successivamente ogni due anni, ai fini del riesame di cui all'articolo 40, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni e raccomandazioni sulla base del risultato delle revisioni tra pari di cui all'articolo 19, che sono effettuate in relazione ai CSIRT nazionali. Tale relazione è trasmessa al gruppo di cooperazione.

5. La rete di CSIRT adotta il proprio regolamento interno.

6. La rete di CSIRT ed EU-CyCLONe concordano le modalità procedurali e cooperano su tale base.

Articolo 16

Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)

1. EU-CyCLONe è istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi in cui un incidente di cibersicurezza su vasta scala potenziale o in corso abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della presente direttiva, della Commissione. Negli altri casi, la Commissione partecipa alle attività di EU-CyCLONe in qualità di osservatore.

L'ENISA assicura il segretariato di EU-CyCLONe e sostiene lo scambio sicuro di informazioni, oltre a fornire gli strumenti necessari per sostenere la cooperazione tra gli Stati membri garantendo uno scambio sicuro di informazioni.

Ove opportuno, EU-CyCLONe può invitare i rappresentanti dei pertinenti portatori di interessi a partecipare ai suoi lavori in qualità di osservatori.

3. EU-CyCLONe svolge i compiti seguenti:

a) aumentare il livello di preparazione per la gestione di crisi e incidenti su vasta scala;

b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi di cibersicurezza su vasta scala;

c) valutare le conseguenze e l'impatto dei pertinenti incidenti e delle pertinenti crisi di cibersicurezza su vasta scala e proporre possibili misure di attenuazione;

d) coordinare la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e sostenere il processo decisionale a livello politico in merito a tali incidenti e crisi;

e) discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4.

4. EU-CyCLONe adotta il proprio regolamento interno.

5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito alla gestione degli incidenti e delle crisi di cibersicurezza su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti.

6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate previste all'articolo 15, paragrafo 6.

7. Entro il 17 luglio 2024 e successivamente ogni 18 mesi, EU-CyCLONe presenta al Parlamento europeo e al Consiglio una relazione di valutazione del proprio lavoro.

Articolo 17

Cooperazione internazionale

Ove opportuno, l'Unione può concludere accordi internazionali, conformemente all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi sono conformi al diritto dell'Unione in materia di protezione dei dati.

Articolo 18

Relazione sullo stato della cibersicurezza nell'Unione

1. L'ENISA, in collaborazione con la Commissione e con il gruppo di cooperazione, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione e la presenta al Parlamento europeo. La relazione è resa disponibile, fra l'altro, in un formato leggibile meccanicamente e comprende gli aspetti seguenti:

a) una valutazione del rischio di cibersicurezza a livello dell'Unione, che tenga conto del panorama delle minacce informatiche;

b) una valutazione dello sviluppo delle capacità di cibersicurezza nei settori pubblico e privato nell'Unione;

c) una valutazione del livello generale di consapevolezza in materia di cibersicurezza e di igiene informatica tra i cittadini e i soggetti, comprese le piccole e medie imprese;

d) una valutazione aggregata del risultato delle revisioni tra pari di cui all'articolo 19;

e) una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersicurezza nell'Unione, comprese quelle a livello settoriale, nonché del livello di allineamento delle strategie nazionali di cibersicurezza degli Stati membri.

2. La relazione contiene raccomandazioni strategiche specifiche, finalizzate a porre rimedio alle carenze e ad aumentare il livello di cibersicurezza nell'Unione, e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione per quanto riguarda gli incidenti e le minacce informatiche, elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881.

3. L'ENISA, in collaborazione con la Commissione, il gruppo di cooperazione e la rete di CSIRT, elabora la metodologia, ivi comprese le variabili pertinenti — come ad esempio indicatori quantitativi e qualitativi — della valutazione aggregata di cui al paragrafo 1, lettera e).

Articolo 19

Revisioni tra pari

1. Con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT ed entro il 17 gennaio 2025, il gruppo di cooperazione stabilisce la metodologia e gli aspetti organizzativi delle revisioni tra pari con l'obiettivo di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità e le politiche di cibersicurezza degli Stati membri necessarie per attuare la presente direttiva. La partecipazione alle revisioni tra pari è volontaria. Le revisioni tra pari sono condotte da esperti di cibersicurezza. Gli esperti di cibersicurezza sono designati da almeno due Stati membri, diversi dallo Stato membro oggetto di revisione.

Le revisioni tra pari riguardano almeno uno degli aspetti seguenti:

a) il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza enunciate agli articoli 21 e 23;

b) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti delle autorità competenti;

c) le capacità operative dei CSIRT;

d) il livello di attuazione dell'assistenza reciproca di cui all'articolo 37;

e) il livello di attuazione degli accordi per la condivisione delle informazioni in materia di cibersicurezza di cui all'articolo 29;

f) le questioni specifiche di natura transfrontaliera o intersettoriale.

2. La metodologia di cui al paragrafo 1 comprende criteri obiettivi, non discriminatori, equi e trasparenti sulla base dei quali gli Stati membri designano esperti di cibersicurezza idonei a eseguire le revisioni tra pari. La Commissione e l'ENISA partecipano alle revisioni tra pari in qualità di osservatori.

3. Gli Stati membri possono individuare questioni specifiche di cui al paragrafo 1, lettera f), ai fini di una revisione tra pari.

4. Prima dell'inizio di una revisione tra pari di cui al paragrafo 1, gli Stati membri notificano agli Stati membri partecipanti il suo ambito di applicazione, comprese le questioni specifiche individuate ai sensi del paragrafo 3.

5. Prima dell'inizio della revisione tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti oggetto della revisione e fornire tale autovalutazione agli esperti di cibersicurezza designati. Il gruppo di cooperazione, con l'assistenza della Commissione e dell'ENISA, stabilisce la metodologia per l'autovalutazione degli Stati membri.

6. Le revisioni tra pari comportano visite in loco fisiche o virtuali e scambi di informazioni a distanza. In linea con il principio di buona collaborazione, lo Stato membro sottoposto alla revisione tra pari fornisce agli esperti di cibersicurezza designati le informazioni necessarie per la valutazione, fatta salva la legislazione nazionale o dell'Unione in materia di protezione di informazioni riservate o classificate e di salvaguardia delle funzioni essenziali dello Stato, quali la sicurezza nazionale. Il gruppo di cooperazione, in collaborazione con la Commissione e con l'ENISA, elabora codici di condotta adeguati, su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati. Le informazioni ottenute mediante la revisione tra pari sono utilizzate unicamente a tal fine. Gli esperti di cibersicurezza che partecipano alla revisione tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso di tale revisione tra pari.

7. Una volta sottoposti a revisione tra pari, i medesimi aspetti esaminati in uno Stato membro non sono più soggetti a ulteriori revisioni tra pari in tale Stato membro per i due anni successivi alla conclusione della revisione, a meno che non sia diversamente richiesto o stabilito dallo Stato membro su proposta del gruppo di cooperazione.

8. Gli Stati membri provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti di cibersicurezza designati siano rivelati agli altri Stati membri, al gruppo di cooperazione, alla Commissione e all'ENISA prima dell'inizio della revisione tra pari. Lo Stato membro che è sottoposto alla revisione tra pari può opporsi alla designazione di particolari esperti di cibersicurezza per motivi debitamente giustificati, comunicati allo Stato membro designante.

9. Gli esperti di cibersicurezza che partecipano alle revisioni tra pari elaborano relazioni sui risultati e sulle conclusioni delle revisioni tra pari. Gli Stati membri sottoposti a revisione tra pari possono formulare osservazioni sui progetti di relazione che li riguardano e tali osservazioni sono allegate alle relazioni. Le relazioni contengono raccomandazioni che consentono di migliorare gli aspetti sottoposti alla revisione tra pari. Le relazioni sono presentate al gruppo di cooperazione e alla rete di CSIRT, se del caso. Uno Stato membro sottoposto alla revisione tra pari può decidere di rendere pubblica la sua relazione o una sua versione espunta.

CAPO IV

MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE

Articolo 20

Governance

1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo.

L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

Articolo 21

Misure di gestione dei rischi di cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

3. Gli Stati membri provvedono affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), del presente articolo, siano adeguate, i soggetti tengano conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Gli Stati membri provvedono inoltre affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), siano adeguate, i soggetti siano tenuti a tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1.

4. Gli Stati membri provvedono affinché, qualora un soggetto constati di non essere conforme alle misure di cui al paragrafo 2, esso adotti, senza indebito ritardo, tutte le misure correttive necessarie, appropriate e proporzionate.

5. Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure di cui al paragrafo 2 per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari.

La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di cui al paragrafo 2 per quanto riguarda i soggetti essenziali e importanti diversi da quelli di cui al primo comma del presente paragrafo.

Nell'elaborare gli atti di esecuzione di cui al primo e secondo comma del presente paragrafo, la Commissione segue, nella misura del possibile, le norme europee e internazionali, nonché le pertinenti specifiche tecniche. La Commissione scambia pareri e coopera con il gruppo di cooperazione e con l'ENISA in merito ai progetti di atto di esecuzione conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 22

Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi TIC, sistemi TIC o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, nonché, ove necessario, dei pertinenti portatori di interessi, identifica i servizi TIC, i sistemi TIC o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata del rischio per la sicurezza di cui al paragrafo 1.

Articolo 23

Obblighi di segnalazione

1. Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al paragrafo 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al paragrafo 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Ciascuno Stato membro provvede affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità.

Qualora i soggetti interessati notifichino all'autorità competente un incidente significativo conformemente al primo comma, lo Stato membro provvede affinché l'autorità competente inoltri la notifica al CSIRT dopo averla ricevuta.

In caso di incidente significativo transfrontaliero o intersettoriale, gli Stati membri provvedono affinché i loro punti di contatto unici ricevano in tempo utile informazioni pertinenti notificate conformemente al paragrafo 4.

2. Se opportuno, gli Stati membri provvedono affinché i soggetti essenziali e importanti comunichino senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia. Se opportuno, i soggetti informano tali destinatari anche della minaccia informatica significativa stessa.

3. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

   i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

   ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

   iii) le misure di attenuazione adottate e in corso;

   iv) se opportuno, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

In deroga al primo comma, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, informa il CSIRT o, se opportuno, l'autorità competente senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

5. Senza indebito ritardo e ove possibile entro 24 ore dal ricevimento del preallarme di cui al paragrafo 4, lettera a), il CSIRT o l'autorità competente fornisce una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza operativa sull'attuazione di possibili misure di attenuazione. Se il CSIRT non è il destinatario iniziale della notifica di cui al paragrafo 1, gli orientamenti sono forniti dall'autorità competente in cooperazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT o l'autorità competente fornisce anche orientamenti sulla segnalazione dell'incidente significativo alle autorità di contrasto.

6. Se opportuno, e in particolare se l'incidente significativo interessa due o più Stati membri, il CSIRT, l'autorità competente o il punto di contatto unico ne informa senza indebito ritardo gli altri Stati membri interessati e l'ENISA. Tali informazioni includono o il tipo di informazioni ricevute a norma del paragrafo 4. Nel fare ciò, il CSIRT, l'autorità competente o il punto di contatto unico tutelano, in conformità al diritto dell'Unione o nazionale, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite.

7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato il CSIRT di uno Stato membro o, se del caso, la sua autorità competente e, se opportuno, i CSIRT o le autorità competenti degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al soggetto di farlo.

8. Su richiesta del CSIRT o dell'autorità competente, il punto di contatto unico inoltra le notifiche ricevute a norma del paragrafo 1 ai punti di contatto unici degli altri Stati membri interessati.

9. Il punto di contatto unico trasmette ogni tre mesi all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può adottare orientamenti tecnici sui parametri delle informazioni da includere nella relazione di sintesi. Ogni sei mesi l'ENISA informa il gruppo di cooperazione e la rete di CSIRT delle sue constatazioni in merito alle notifiche ricevute.

10. I CRSIRT o, se opportuno, le autorità competenti forniscono alle autorità competenti a norma della direttiva (UE) 2022/2557 le informazioni sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30 dai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557.

11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma del paragrafo 1 del presente articolo e dell'articolo 30 e di una comunicazione trasmessa a norma del paragrafo 2 del presente articolo.

Entro il 17 ottobre 2024 la Commissione adotta, per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, nonché i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, atti di esecuzione che specifichino ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. La Commissione può adottare tali atti di esecuzione in relazione ad altri soggetti essenziali e importanti.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo e secondo comma del presente paragrafo conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 24

Uso dei sistemi europei di certificazione della cibersicurezza

1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati.

2. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 38 al fine di integrare la presente direttiva specificando quali categorie di soggetti essenziali e importanti sono tenute a utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881. Tali atti delegati sono adottati qualora siano stati individuati livelli insufficienti di cibersicurezza e includono un periodo di attuazione.

Prima di adottare tali atti delegati, la Commissione effettua una valutazione d'impatto e procede a consultazioni conformemente all'articolo 56 del regolamento (UE) 2019/881.

3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2 del presente articolo, la Commissione può chiedere all'ENISA, previa consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, di preparare una proposta di sistema a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.

Articolo 25

Normazione

1. Per promuovere l'attuazione convergente dell'articolo 21, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informatici e di rete.

2. L'ENISA, in cooperazione con gli Stati membri e, se opportuno, previa consultazione dei pertinenti portatori di interessi, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.

CAPO V

GIURISDIZIONE E REGISTRAZIONE

Articolo 26

Giurisdizione e territorialità

1. I soggetti che rientrano nell'ambito di applicazione della presente direttiva sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:

a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;

b) i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione a norma del paragrafo 2;

c) gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini della presente direttiva, si considera che un soggetto di cui al paragrafo 1, lettera b), abbia il proprio stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione.

3. Se un soggetto di cui al paragrafo 1, lettera b), non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante nell'Unione designato a norma del presente paragrafo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per violazione degli obblighi della presente direttiva.

4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.

5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un soggetto di cui al paragrafo 1, lettera b), possono, entro i limiti della richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che ha un sistema informatico e di rete nel loro territorio.

Articolo 27

Registro dei soggetti

1. L'ENISA crea e mantiene un registro di fornitori di servizi DNS, registri dei nomi di dominio di primo livello, soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti, nonché fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 4. Su richiesta, l'ENISA consente alle autorità competenti di accedere a tale registro, assicurando nel contempo la tutela della riservatezza delle informazioni, se del caso.

2. Gli Stati membri esigono che i soggetti di cui al paragrafo 1 trasmettano entro il 17 gennaio 2025, le informazioni seguenti alle autorità competenti:

a) il proprio nome;

b) il settore, il sottosettore e il tipo di soggetto di cui all'allegato I o II, se del caso;

c) l'indirizzo dello stabilimento principale e degli altri stabilimenti legali del soggetto nell'Unione o, se non è stabilito nell'Unione, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

d) i dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono del soggetto, e, se opportuno, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

e) gli Stati membri in cui il soggetto fornisce i suoi servizi; e

f) le serie di IP del soggetto.

3. Gli Stati membri provvedono affinché i soggetti di cui al paragrafo 1 notifichino all'autorità competente qualsiasi modifica dei dettagli trasmessi a norma del paragrafo 2 tempestivamente e, in ogni caso, entro tre mesi dalla data della modifica.

4. In seguito alla ricezione delle informazioni di cui ai paragrafi 2 e 3, ad eccezione di quelle di cui al paragrafo 2, lettera f), il punto di contatto unico dello Stato membro interessato, senza ritardo, le inoltra all'ENISA.

5. Se opportuno, le informazioni di cui ai paragrafi 2 e 3 del presente articolo sono trasmesse attraverso il meccanismo nazionale di cui all'articolo 3, paragrafo 4, quarto comma.

Articolo 28

Banca dati dei dati di registrazione dei nomi di dominio

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri impongono ai registri dei nomi di TLD e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di raccogliere e mantenere dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali.

2. Ai fini del paragrafo 1, gli Stati membri esigono che la banca dati dei dati di registrazione dei nomi di dominio contenga le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD. Tali informazioni includono:

a) il nome di dominio;

b) la data di registrazione;

c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione;

d) l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.

3. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio predispongano politiche e procedure, incluse procedure di verifica, per garantire che le banche dati di cui al paragrafo 1 comprendano informazioni accurate e complete. Gli Stati membri esigono che tali politiche e procedure siano rese pubbliche.

4. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rendano pubblicamente disponibili, senza indebito ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.

5. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio, su richiesta legittima e debitamente motivata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo e comunque entro 72 ore dalla ricezione delle richieste di accesso. Gli Stati membri esigono che le politiche e le procedure relative alla divulgazione di tali dati siano rese pubbliche.

6. Il rispetto degli obblighi di cui ai paragrafi da 1 a 5 non comportano una duplicazione della raccolta di dati di registrazione dei nomi di dominio. A tal fine, gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio collaborino tra loro.

CAPO VI

CONDIVISIONE DELLE INFORMAZIONI

Articolo 29

Accordi di condivisione delle informazioni sulla cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti che rientrano nell'ambito di applicazione della presente direttiva e, se del caso, altri soggetti che non rientrano nell'ambito di applicazione della presente direttiva siano in grado di scambiarsi, su base volontaria, pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche, se tale condivisione di informazioni:

a) mira a prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto;

b) aumenta il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità di soggetti essenziali e importanti e, se opportuno, dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di condivisione delle informazioni sulla cibersicurezza che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

3. Gli Stati membri facilitano la conclusione degli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 del presente articolo. Gli Stati membri possono specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, gli Stati membri possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT. Gli Stati membri offrono assistenza per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 7, paragrafo 2, lettera h).

4. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. L'ENISA offre assistenza per la conclusione di accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 fornendo orientamenti e provvedendo allo scambio delle migliori pratiche.

Articolo 30

Notifica volontaria di informazioni pertinenti

1. Gli Stati membri provvedono affinché, in aggiunta all'obbligo di notifica di cui all'articolo 23, possano essere trasmesse, su base volontaria, notifiche ai CSIRT o, se opportuno, alle autorità competenti, da parte dei:

a) soggetti essenziali e importanti, per quanto riguarda gli incidenti, le minacce informatiche e i quasi incidenti;

b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, per quanto riguarda gli incidenti significativi, le minacce informatiche e i quasi incidenti.

2. Gli Stati membri trattano le notifiche di cui al paragrafo 1 del presente articolo secondo la procedura di cui all'articolo 23. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie.

Se necessario, i CSIRT e, se del caso, le autorità competenti forniscono ai punti di contatto unici le informazioni sulle notifiche ricevute a norma del presente articolo, garantendo nel contempo la riservatezza e la tutela adeguata delle informazioni fornite dal soggetto notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre al soggetto notificante alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

CAPO VII

VIGILANZA ED ESECUZIONE

Articolo 31

Aspetti generali relativi alla vigilanza e all'esecuzione

1. Gli Stati membri provvedono affinché le proprie autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva.

2. Gli Stati membri possono consentire alle proprie autorità competenti di conferire priorità ai compiti di vigilanza. Tale priorità si fonda su un approccio basato sul rischio. A tal fine, nell'esercizio dei rispettivi compiti di vigilanza di cui agli articoli 32 e 33, le autorità competenti possono stabilire metodologie di vigilanza che consentano di conferire priorità a tali compiti secondo un approccio basato sul rischio.

3. Le autorità competenti operano in stretta cooperazione con le autorità di controllo ai sensi del regolamento (UE) 2016/679 nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti delle autorità di controllo di cui a tale regolamento.

4. Fatti salvi i quadri legislativi e istituzionali nazionali, gli Stati membri provvedono affinché nel vigilare sul rispetto, da parte degli enti della pubblica amministrazione, della presente direttiva e nell'imporre misure di esecuzione in caso di violazione della presente direttiva, le autorità competenti dispongano dei poteri adeguati per svolgere tali compiti con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza. Gli Stati membri possono decidere di imporre misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti conformemente ai quadri legislativi e istituzionali nazionali.

Articolo 32

Misure di vigilanza e di esecuzione relative a soggetti essenziali

1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a:

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;

b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;

c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della presente direttiva da parte del soggetto essenziale;

d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;

g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto ad audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettera e), f) o g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le proprie autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere come minimo di:

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti, ivi incluso per quanto riguarda le misure richieste per evitare il verificarsi di un incidente o porvi rimedio, nonché i termini per l'attuazione di tali misure e per riferire in merito alla loro attuazione, o un'ingiunzione che impongano ai soggetti interessati di porre rimedio alle carenze individuate o alle violazioni della direttiva;

c) imporre ai soggetti interessati di porre termine al comportamento che viola la presente direttiva e di astenersi dal ripeterlo;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione del rischio di cibersicurezza siano conformi all'articolo 21 o di adempiere gli obblighi di segnalazione di cui all'articolo 23 in una maniera ed entro un termine specificati;

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia, nonché in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre ai soggetti interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato al fine di vigilare sul rispetto degli articoli 18 e 20;

h) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo il diritto nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a qualsiasi delle misure di cui al presente paragrafo, lettere da a) a h).

5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di:

a) sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale;

b) chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto.

Le sospensioni o i divieti temporanei a norma del presente paragrafo sono applicati solo finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le misure di esecuzione sono state applicate. L'imposizione di tali sospensioni o divieti temporanei è soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad un giusto processo, la presunzione di innocenza e i diritti della difesa.

Le misure di esecuzione previste dal presente paragrafo non sono applicabili agli enti della pubblica amministrazione che sono soggetti alla presente direttiva.

6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia il potere di garantirne il rispetto della presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto della presente direttiva.

Per quanto riguarda gli enti della pubblica amministrazione, il presente paragrafo lascia impregiudicato il diritto nazionale in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

7. Nell'adottare qualsiasi misura di esecuzione di cui al paragrafo 4 o 5, le autorità competenti rispettano i diritti della difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

a) la gravità della violazione e l'importanza delle disposizioni violate, essendo le violazioni seguenti, tra l'altro, da considerarsi gravi:

   i) le violazioni ripetute;

   ii) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;

   iii) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti;

   iv) l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione;

   v) la fornitura di informazioni false o gravemente inesatte relative alle misure in materia di gestione o segnalazione del rischio di cibersicurezza di cui agli articoli 21 e 23;

b) la durata della violazione;

c) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;

d) qualsiasi danno materiale o immateriale causato, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati;

e) un'eventuale condotta intenzionale o negligenza da parte dell'autore della violazione;

f) qualsiasi misure adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale;

g) qualsiasi adesione a codici di condotta o meccanismi di certificazione approvati;

h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti.

8. Le autorità competenti espongono nei particolari la motivazione delle loro misure di esecuzione. Prima di adottare tali misure le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Esse concedono inoltre a tali soggetti un tempo ragionevole per presentare osservazioni, salvo in casi debitamente giustificati in cui ciò impedirebbe di agire con immediatezza per prevenire un incidente o rispondervi.

9. Gli Stati membri provvedono affinché le loro autorità competenti di cui alla presente direttiva informino le autorità competenti pertinenti all'interno dello stesso Stato membro a norma della direttiva (UE) 2022/2557 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto identificato come critico a norma della direttiva (UE) 2022/2557. Se del caso, le autorità competenti di cui alla direttiva (UE) 2022/2557 possono chiedere alle autorità competenti di cui alla presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è stato individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557.

10. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554

Articolo 33

Vigilanza ed esecuzione relative a soggetti essenziali

1. Se ricevono elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la presente direttiva, in particolare dagli articoli 21 e 23 della medesima, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post. Gli Stati membri provvedono affinché tali misure siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a:

a) ispezioni in loco e vigilanza ex post a distanza, effettuate da professionisti formati;

b) audit sulla sicurezza mirati svolti da un organismo indipendente o da un'autorità competente;

c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario, con la cooperazione del soggetto interessato;

(d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di gestione dei rischi di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei propri compiti di vigilanza;

f) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto a audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere d), e) o f), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere come minimo di:

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi della presente direttiva;

c) imporre ai soggetti interessati di porre termine alle condotte in violazione della presente direttiva e di astenersi dal ripeterle;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione dei rischi di cibersicurezza siano conformi all'articolo 21 o i loro obblighi di segnalazione conformi alle prescrizioni di cui all'articolo 23 in una maniera ed entro un termine specificati;

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia e alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre agli interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

h) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo la legislazione nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a una qualsiasi delle misure di cui al presente paragrafo, lettere da a) a g).

5. L'articolo 32, paragrafi 6, 7 e 8, si applica mutatis mutandis alle misure di vigilanza ed esecuzione di cui al presente articolo per soggetti importanti.

6. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto importante designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554.

Articolo 34

Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni della presente direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Le sanzioni amministrative pecuniarie sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g).

3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 32, paragrafo 7.

4. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti essenziali siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

5. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti importanti siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

6. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione della presente direttiva conformemente a una precedente decisione dell'autorità competente.

7. Fatti salvi i poteri delle autorità competenti a norma degli articoli 32 e 33, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione.

8. Se l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Lo Stato membro notifica alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 17 ottobre 2024 e ne comunicano senza ritardo ogni successiva modifica.

Articolo 35

Violazioni che comportano una violazione dei dati personali

1. Qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli articoli 21 e 23 della presente direttiva da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata a norma dell'articolo 33 del medesimo regolamento, ne informano senza indebito ritardo le autorità di controllo competenti a norma dell'articolo 55 o 56 di tale regolamento.

2. Qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della presente direttiva per una violazione di cui al presente articolo, paragrafo 1, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del regolamento (UE) 2016/679. Le autorità competenti possono tuttavia imporre le misure di esecuzione di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g) della presente direttiva.

3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto all'autorità competente, l'autorità competente informa l'autorità di controllo stabilita nel proprio Stato membro della potenziale violazione dei dati personali di cui al paragrafo 1.

Articolo 36

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle misure nazionali adottate in attuazione della presente direttiva e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri comunicano alla Commissione, entro il 17 gennaio 2025, tali norme e misure e la informano, immediatamente, di qualsiasi modifica apportata successivamente.

Articolo 37

Assistenza reciproca

1. Se un soggetto fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e i suoi sistemi informatici e di rete sono ubicati in uno o più altri Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti:

a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate;

b) un'autorità competente può chiedere a un'altra autorità competente di adottare misure di vigilanza o esecuzione;

c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente un'assistenza reciproca proporzionata alle proprie risorse affinché le misure di vigilanza o esecuzione possano essere attuate in maniera efficace, efficiente e coerente.

L'assistenza reciproca di cui al primo comma. Lettera c), può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione e l'ENISA,

2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza comuni.

CAPO VIII

ATTI DELEGATI E ATTI DI ESECUZIONE

Articolo 38

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 24, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 16 gennaio 2023.

3. La delega di potere di cui all'articolo 24, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato a norma dell'articolo 24, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 39

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

CAPO IX

DISPOSIZIONI FINALI

Articolo 40

Riesame

Entro il 17 ottobre 2027 e successivamente ogni 36 mesi, la Commissione riesamina il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza delle dimensioni dei soggetti interessati, e i settori, sottosettori e tipologie di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. A tal fine e allo scopo di intensificare ulteriormente la cooperazione strategica e operativa, la Commissione tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo. La relazione è corredata, se necessario, di una proposta legislativa.

Articolo 41

Recepimento

1. Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Essi applicano tali disposizioni a decorrere dal 18 ottobre 2024.

2. Le disposizioni di cui al paragrafo 1 adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 42

Modifica del regolamento (UE) n. 910/2014

Nel regolamento (UE) n. 910/2014, l'articolo 19 è soppresso con effetto a decorrere dal 18 ottobre 2024.

Articolo 43

Modifica della direttiva (UE) 2018/1972

Nella direttiva (UE) 2018/1972, gli articoli 40 e 41 sono soppressi. con effetto a decorrere dal 18 ottobre 2024.

Articolo 44

Abrogazione

La direttiva (UE) 2016/1148 è abrogata con effetto a decorrere dal 18 ottobre 2024.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva e vanno letti secondo la tavola di concordanza di cui all'allegato III.

Articolo 45

Entrata in vigore

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

Articolo 46

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK

ALLEGATO I

SETTORI AD ALTA CRITICITÀ

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio ([1]) che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio ([2]) — Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944 — Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio ([3])
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio ([4])
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio ([5])
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno

Settore	Sottosettore	Tipo di soggetto
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([6]), aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([7]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([8])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([9])
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio ([10]), escluse le singole navi gestite da tale compagnia
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([11]), compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([12])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione ([13]) responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([14])
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([15])
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([16])
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([17])

Settore	Sottosettore	Tipo di soggetto
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([18])
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio ([19])
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ([20]) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio ([21])
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio ([22]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio ([23]), escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale
8. Infrastrutture digitali		— Fornitori di punti di interscambio internet
		— Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice
		— Registri dei nomi di dominio di primo livello (TLD)
		— Fornitori di servizi di cloud computing
		— Fornitori di servizi di data center
		— Fornitori di reti di distribuzione dei contenuti (content delivery network)
		— Fornitori di servizi fiduciari
		— Fornitori di reti pubbliche di comunicazione
		— Fornitori di servizi di comunicazione elettronica accessibili al pubblico
9. Gestione dei servizi TIC (business-to-business)		— Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti

Settore	Sottosettore	Tipo di soggetto
10. Pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale
		— Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale
11. Spazio		Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

([1]) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).
([2]) Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).
([3]) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).
([4]) Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).
([5]) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
([6]) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
([7]) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
([8]) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
([9]) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
([10]) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).
([11]) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).
([12]) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10)
([13]) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
([14]) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
([15]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).
([16]) 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).
([17]) 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).
([18]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

([19]) Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).

([20]) Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).

([21]) Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici (GU L 20 del 31.1.2022, pag. 1).

([22]) Direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio del 16 dicembre 2020 concernente la qualità delle acque destinate al consumo umano (GU L 435 del 23.12.2020, pag. 1).

([23]) Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).

ALLEGATO II

ALTRI SETTORI CRITICI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 *bis*), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio ([1]), escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio ([2]) e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio ([3]) che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio ([4]) e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ([5]) ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2

Settore	Sottosettore	Tipo di soggetto
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network
7. Ricerca		Organizzazioni di ricerca

([1]) Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).

([2]) Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE (GU L 396 del 30.12.2006, pag. 1).

([3]) Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 dell'1.2.2002, pag. 1).

([4]) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

([5]) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

ALLEGATO III

TAVOLA DI CONCORDANZA

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 1, paragrafo 1	Articolo 1, paragrafo 1
Articolo 1, paragrafo 2	Articolo 1, paragrafo 2
Articolo 1, paragrafo 3	—
Articolo 1, paragrafo 4	Articolo 2, paragrafo 12
Articolo 1, paragrafo 5	Articolo 2, paragrafo 13
Articolo 1, paragrafo 6	Articolo 2, paragrafi 6 e 11
Articolo 1, paragrafo 7	Articolo 4
Articolo 2	Articolo 2, paragrafo 14
Articolo 3	Articolo 5
Articolo 4	Articolo 6
Articolo 5	—
Articolo 6	—
Articolo 7, paragrafo 1	Articolo 7, paragrafi 1 e 2
Articolo 7, paragrafo 2	Articolo 7, paragrafo 4
Articolo 7, paragrafo 3	Articolo 7, paragrafo 3
Articolo 8, paragrafi da 1 a 5	Articolo 8, paragrafi da 1 a 5
Articolo 8, paragrafo 6	Articolo 13, paragrafo 4
Articolo 8, paragrafo 7	Articolo 8, paragrafo 6
Articolo 9, paragrafi 1, 2 e 3	Articolo 10, paragrafi 1, 2 e 3
Articolo 9, paragrafo 4	Articolo 10, paragrafo 9
Articolo 9, paragrafo 5	Articolo 10, paragrafo 10
Articolo 10, paragrafi 1, 2 e 3, primo comma	Articolo 13, paragrafi 1, 2 e 3
Articolo 10, paragrafo 3, secondo comma	Articolo 23, paragrafo 9
Articolo 11, paragrafo 1	Articolo 14, paragrafi 1 e 2
Articolo 11, paragrafo 2	Articolo 14, paragrafo 3
Articolo 11, paragrafo 3	Articolo 14, paragrafo 4, primo comma, lettere da a) a q) e s), e paragrafo 7
Articolo 11, paragrafo 4	Articolo 14, paragrafo 4, primo comma, lettera r), e secondo comma
Articolo 11, paragrafo 5	Articolo 14, paragrafo 8
Articolo 12, paragrafi da 1 a 5	Articolo 15, paragrafi da 1 a 5
Articolo 13	Articolo 17
Articolo 14, paragrafi 1 e 2	Articolo 21, paragrafi da 1 a 4
Articolo 14, paragrafo 3	Articolo 23, paragrafo 1
Articolo 14, paragrafo 4	Articolo 23, paragrafo 3
Articolo 14, paragrafo 5	Articolo 23, paragrafi 5, 6 e 8

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 14, paragrafo 6	Articolo 23, paragrafo 7
Articolo 14, paragrafo 7	Articolo 23, paragrafo 11
Articolo 15, paragrafo 1	Articolo 31, paragrafo 1
Articolo 15, paragrafo 2, primo comma, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 15, paragrafo 2, primo comma, lettera b)	Articolo 32, paragrafo 2, lettera g)
articolo 15, paragrafo 2, secondo comma	Articolo 32, paragrafo 3
Articolo 15, paragrafo 3	Articolo 32, paragrafo 4, lettera b)
Articolo 15, paragrafo 4	Articolo 31, paragrafo 3
Articolo 16, paragrafi 1 e 2	Articolo 21, paragrafi da 1 e 4
Articolo 16, paragrafo 3	Articolo 23, paragrafo 1
Articolo 16, paragrafo 4	Articolo 23, paragrafo 3
Articolo 16, paragrafo 5	—
Articolo 16, paragrafo 6	Articolo 23, paragrafo 6
Articolo 16, paragrafo 7	Articolo 23, paragrafo 7
Articolo 16, paragrafi 8 e 9	Articolo 21, paragrafo 5, e articolo 23, paragrafo 11
Articolo 16, paragrafo 10	—
Articolo 16, paragrafo 11	Articolo 2, paragrafi 1, 2 e 3
Articolo 17, paragrafo 1	-Articolo 33, paragrafo 1
Articolo 17, paragrafo 2, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 17, paragrafo 2, lettera b)	Articolo 32, paragrafo 4, lettera b)
Articolo 17, paragrafo 3	Articolo 37, paragrafo 1, lettere a) e b)
Articolo 18, paragrafo 1	Articolo 26, paragrafo 1, lettera b), e paragrafo 2
Articolo 18, paragrafo 2	Articolo 26, paragrafo 3
Articolo 18, paragrafo 3	Articolo 26, paragrafo 4
Articolo 19	Articolo 25
Articolo 20	Articolo 30
Articolo 21	Articolo 36
Articolo 22	Articolo 39
Articolo 23	Articolo 40
Articolo 24	—
Articolo 25	Articolo 41
Articolo 26	Articolo 45
Articolo 27	Articolo 46
Allegato I, punto 1	Articolo 11, paragrafo 1
Allegato I, punto 2, lettera a), punti da i) a iv)	Articolo 11, paragrafo 2, lettere da a) a d)

Direttiva (UE) 2016/1148	Presente direttiva
Allegato I, punto 2, lettera a), punto v)	Articolo 11, paragrafo 2, lettera f)
Allegato I, punto 2, lettera b)	Articolo 11, paragrafo 4
Allegato I, punto 2, lettera c), punti i) e ii)	Articolo 11, paragrafo 5, lettera a)
Allegato II	Allegato I
Allegato III, punti 1 e 2	Allegato II, punto 6
Allegato III, punto 3	Allegato I, punto 8

DIRETTIVA (UE) 2022/2556 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 53, paragrafo 1, e l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea ([1]),

visto il parere del Comitato economico e sociale europeo ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) L'Unione deve affrontare in modo adeguato e completo i rischi digitali cui sono esposte tutte le entità finanziarie a causa di un maggiore uso delle tecnologie dell'informazione e della comunicazione (TIC) nella fornitura e nel consumo di servizi finanziari, contribuendo così alla realizzazione del potenziale della finanza digitale in termini di stimolazione dell'innovazione e promozione della concorrenza in un ambiente digitale sicuro.

(2) Le entità finanziarie dipendono fortemente dall'uso delle tecnologie digitali nella loro attività quotidiana. È pertanto essenziale garantire la resilienza operativa delle loro operazioni digitali a fronte dei rischi informatici. Tale necessità è diventata ancora più pressante a causa della crescita delle tecnologie innovative nel mercato, in particolare le tecnologie che consentono di trasferire e archiviare elettronicamente le rappresentazioni digitali di valore o di diritti utilizzando il registro distribuito o tecnologie analoghe (cripto-attività), nonché della crescita dei servizi connessi a tali attività.

([1]) GU C 343 del 26.8.2021, pag. 1.
([2]) GU C 155 del 30.4.2021, pag. 38.
([3]) Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.

(3) A livello di Unione, i requisiti connessi alla gestione dei rischi informatici nel settore finanziario sono attualmente previsti dalle direttive 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) e (UE) 2016/2341 ([11]) del Parlamento europeo e del Consiglio.

Tali requisiti sono diversi e talvolta incompleti. In alcuni casi, i rischi informatici sono stati affrontati solo implicitamente come parte del rischio operativo e in altri casi non sono stati affrontati affatto. A tale situazione si è posto rimedio con l'adozione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([12]). È pertanto opportuno che tali direttive siano modificate per garantire la coerenza con detto regolamento. La presente direttiva attua una serie di modifiche che sono necessarie per apportare chiarezza giuridica e coerenza in relazione all'applicazione, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza conformemente a tali direttive, dei vari requisiti di resilienza operativa digitale necessari per lo svolgimento delle loro attività e per la prestazione di servizi, garantendo in tal modo il corretto funzionamento del mercato interno. È necessario assicurare l'adeguatezza di tali requisiti agli sviluppi del mercato incoraggiando nel contempo la proporzionalità, in particolare per quanto riguarda le dimensioni delle entità finanziarie e dei regimi specifici ai quali sono soggetti, al fine di ridurre i costi di adeguamento alla normativa.

(4) Nel settore dei servizi bancari, la direttiva 2013/36/UE stabilisce attualmente solo norme generali di governance interna e disposizioni sul rischio operativo contenenti requisiti per i piani di emergenza e di continuità operativa che fungono implicitamente da base per affrontare i rischi informatici. Per affrontare i rischi informatici esplicitamente e chiaramente, è però opportuno modificare i requisiti per i piani di emergenza e di continuità operativa al fine di includere anche piani di continuità operativa e di risposta e ripristino riguardanti i rischi informatici, conformemente agli obblighi stabiliti dal regolamento (UE) 2022/2554 Inoltre, i rischi informatici sono inclusi solo implicitamente, nell'ambito del rischio operativo, nel processo di revisione e valutazione prudenziale (*Supervisory Review and Evaluation process* - SREP) svolto dalle autorità competenti, e i criteri per la sua valutazione sono attualmente definiti negli Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology* - ICT) a norma del processo di revisione e valutazione prudenziale (SREP), emessi dall'Autorità europea di vigilanza (Autorità bancaria europea) (ABE), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([13]). Al fine di fornire chiarezza giuridica e assicurare che le autorità di vigilanza bancaria individuino i rischi informatici e ne monitorino efficacemente la

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([8]) 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).

([9]) 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).

([10]) 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).

([11]) 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).

([12]) 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 (cfr. pagina 1 della presente Gazzetta ufficiale).

([13]) 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).

gestione da parte delle entità finanziarie, in linea con il nuovo quadro sulla resilienza operativa digitale, l'ambito di applicazione dello SREP dovrebbe essere modificato anche per fare riferimento esplicitamente agli obblighi stabiliti dal regolamento (UE) 2022/2554 e coprire in particolare i rischi evidenziati dalle segnalazioni di incidenti gravi connessi alle TIC e dai risultati delle verifiche della resilienza operativa digitale effettuate dalle entità finanziarie conformemente a tale regolamento.

(5) La resilienza operativa digitale è fondamentale per preservare le funzioni essenziali e le linee di business principali di un'entità finanziaria in caso di risoluzione ed evitare in tal modo di perturbare l'economia reale e il sistema finanziario. Gli incidenti operativi gravi possono ostacolare la capacità di un'entità finanziaria di continuare a operare e possono compromettere gli obiettivi della risoluzione. Taluni accordi contrattuali per l'utilizzo di servizi TIC sono essenziali per garantire la continuità operativa e fornire i dati necessari in caso di risoluzione. Al fine di rispettare gli obiettivi del quadro dell'Unione per la resilienza operativa, la direttiva 2014/59/UE dovrebbe essere modificata di conseguenza per garantire che le informazioni relative alla resilienza operativa siano prese in considerazione nel contesto della pianificazione della risoluzione e della valutazione della possibilità di risoluzione delle entità finanziarie.

(6) La direttiva 2014/65/UE stabilisce norme più rigorose in materia di rischi informatici per le imprese di investimento e le sedi di negoziazione che effettuano negoziazioni algoritmiche. Requisiti meno dettagliati si applicano ai servizi di comunicazione dei dati e ai repertori di dati sulle negoziazioni. Inoltre, la direttiva 2014/65/UE contiene solo riferimenti limitati ai dispositivi di controllo e di salvaguardia per sistemi di elaborazione delle informazioni e all'uso di sistemi, risorse e procedure adeguati per garantire la continuità e la regolarità dei servizi alle imprese. Inoltre, tale direttiva dovrebbe essere allineata al regolamento (UE) 2022/2554 per quanto riguarda la continuità e la regolarità nell'erogazione di servizi e nello svolgimento delle attività di investimento, la resilienza operativa, la capacità dei sistemi di negoziazione e l'efficacia dei dispositivi di continuità operativa e della gestione del rischio.

(7) La direttiva (UE) 2015/2366 stabilisce norme specifiche per quanto riguarda le misure di controllo e di mitigazione in materia di sicurezza delle TIC ai fini di ottenere un'autorizzazione a erogare servizi di pagamento. È opportuno modificare tali norme in materia di autorizzazione per allinearle al regolamento (UE) 2022/2554 Inoltre, al fine di ridurre gli oneri amministrativi ed evitare la complessità e la duplicazione degli obblighi di segnalazione, le norme in materia di segnalazione degli incidenti di cui a tale direttiva dovrebbero cessare di applicarsi ai prestatori di servizi di pagamento disciplinati da tale direttiva e soggetti al regolamento (UE) 2022/2554 in modo da permettere a tali prestatori di servizi di pagamento di beneficiare di un meccanismo unico, pienamente armonizzato di notifica degli incidenti per tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti, indipendentemente dal fatto che si tratti di incidenti connessi alle TIC.

(8) Le direttive 2009/138/CE e (UE) 2016/2341 tengono parzialmente conto dei rischi informatici nelle rispettive disposizioni generali in materia di governance e gestione del rischio, lasciando che determinati requisiti siano specificati mediante atti delegati con o senza riferimenti specifici ai rischi informatici. Analogamente, ai gestori di fondi di investimento alternativi soggetti alla direttiva 2011/61/UE e alle società di gestione soggette alla direttiva 2009/65/CE si applicano soltanto norme molto generali. È pertanto opportuno allineare tali direttive agli obblighi stabiliti nel regolamento (UE) 2022/2554 per quanto riguarda la gestione dei sistemi e degli strumenti TIC.

(9) In molti casi, ulteriori requisiti in materia di rischi informatici sono già stati stabiliti in atti delegati e di esecuzione, adottati sulla base di progetti di norme tecniche di regolamentazione e di attuazione elaborati dalla competente autorità europea di vigilanza. Dato che le disposizioni del regolamento (UE) 2022/2554 costituiscono la base giuridica in materia di rischi informatici nel settore finanziario, è opportuno modificare determinate competenze ad adottare atti delegati e di esecuzione di cui alle direttive 2009/65/CE, 2009/138/CE, 2011/61/UE e 2014/65/EU al fine di eliminare le disposizioni in materia di rischi informatici dall'ambito di applicazione di tali competenze.

(10) Al fine di garantire un'attuazione coerente del nuovo quadro sulla resilienza operativa digitale per il settore finanziario, gli Stati membri dovrebbero applicare le disposizioni di diritto nazionale che recepiscono la presente direttiva a decorrere dalla data di applicazione del regolamento (UE) 2022/2554

(11) Le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 sono state adottate sulla base dell'articolo 53, paragrafo 1, o dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE) o di entrambi. Le modifiche contenute nella presente direttiva sono state incluse in un unico atto legislativo a causa dell'interconnessione dell'oggetto e degli obiettivi delle modifiche. Di conseguenza, la presente direttiva dovrebbe essere adottata sulla base dell'articolo 53, paragrafo 1, e dell'articolo 114 TFUE.

(12) Poiché gli obiettivi della presente direttiva non possono essere conseguiti in misura sufficiente dagli Stati membri in quanto comportano l'armonizzazione degli obblighi già contenuti nelle direttive ma, a motivo della portata e degli effetti dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(13) Conformemente alla dichiarazione politica comune del 28 settembre 2011 degli Stati membri e della Commissione sui documenti esplicativi ([14]), gli Stati membri si sono impegnati ad accompagnare, in casi giustificati, la notifica delle loro misure di recepimento con uno o più documenti che chiariscano il rapporto tra gli elementi costitutivi di una direttiva e le parti corrispondenti degli strumenti nazionali di recepimento. Per quanto riguarda la presente direttiva, il legislatore ritiene che la trasmissione di tali documenti sia giustificata,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Modifiche della direttiva 2009/65/CE

Il testo dell'articolo 12 della direttiva 2009/65/CE è così modificato:

1) al paragrafo 1, secondo comma, la lettera a) è sostituita dalla seguente:

«a) abbia una buona organizzazione amministrativa e contabile, meccanismi di controllo e di salvaguardia in materia di elaborazione elettronica dei dati, anche per quanto riguarda sistemi informatici e di rete istituiti e gestiti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché procedure adeguate di controllo interno che comprendano, in particolare, regole per le operazioni personali dei dipendenti o per la detenzione o la gestione di investimenti in strumenti finanziari a scopo di investimento in conto proprio e che assicurino, quanto meno, che qualunque transazione in cui intervenga l'OICVM possa essere ricostruita per quanto riguarda l'origine, le controparti, la natura nonché il luogo e il momento in cui è stata effettuata e che il patrimonio degli OICVM gestito dalla società di gestione sia investito conformemente al regolamento del fondo o al suo atto costitutivo e alle norme in vigore;

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

2) il paragrafo 3 è sostituito dal seguente:

«3. Fatto salvo l'articolo 116, la Commissione adotta, mediante atti delegati conformemente all'articolo 112 *bis*, misure che precisano:

a) le procedure e le disposizioni di cui al paragrafo 1, secondo comma, lettera a), diverse dalle procedure e dagli strumenti relativi ai sistemi informatici e di rete;

b) le strutture e i requisiti organizzativi volti a ridurre al minimo i conflitti di interesse di cui al paragrafo 1, secondo comma, lettera b).».

([14]) GU C 369 del 17.12.2011, pag. 14.

Articolo 2

Modifiche della direttiva 2009/138/CE

La direttiva 2009/138/CE è così modificata:

1) all'articolo 41, il paragrafo 4 è sostituito dal seguente:

«4. Le imprese di assicurazione e di riassicurazione adottano misure ragionevoli atte a garantire la continuità e la regolarità dello svolgimento delle loro attività, tra cui l'elaborazione di piani di emergenza. A tal fine, le imprese in questione utilizzano sistemi, risorse e procedure adeguati e proporzionati e, in particolare, istituiscono e gestiscono sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

2) all'articolo 50, paragrafo 1, le lettere a) e b) sono sostituite dalle seguenti:

«a) gli elementi dei sistemi di cui all'articolo 41, all'articolo 44, in particolare i settori elencati all'articolo 44, paragrafo 2, e agli articoli 46 e 47, diversi dagli elementi relativi alla gestione dei rischi informatici;

b) le funzioni di cui agli articoli 44, 46, 47 e 48, diverse dalle funzioni relative alla gestione dei rischi informatici.».

Articolo 3

Modifica della direttiva 2011/61/UE

L'articolo 18 della direttiva 2011/61/UE è sostituito dal seguente:

«*Articolo 18*

Principi generali

1. Gli Stati membri impongono ai GEFIA di ricorrere in ogni momento a risorse umane e tecniche adeguate e adatte per la buona gestione dei FIA.

In particolare, le autorità competenti dello Stato membro d'origine del GEFIA, considerata anche la natura del FIA gestito dal GEFIA, impongono a quest'ultimo di possedere una buona organizzazione amministrativa e contabile, modalità di controllo e di salvaguardia in materia di elaborazione elettronica dei dati, anche per quanto riguarda i sistemi informatici e di rete istituiti e gestiti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché procedure di controllo interno adeguate che comprendano, in particolare, regole per le operazioni personali dei dipendenti o per la detenzione o la gestione di investimenti a scopo di investimento in conto proprio e che assicurino, quanto meno, che qualunque operazione in cui intervenga il FIA possa essere ricostruita per quanto riguarda l'origine, le parti, la natura nonché il luogo e il momento in cui è stata effettuata e che le attività del FIA gestito dal GEFIA siano investite conformemente al regolamento o ai documenti costitutivi del FIA e alle disposizioni normative in vigore.

2. La Commissione adotta, mediante atti delegati in conformità dell'articolo 56 e alle condizioni di cui agli articoli 57 e 58, misure che specifichino le procedure e le modalità di cui al paragrafo 1 del presente articolo diverse dalle procedure e modalità relative ai sistemi informatici e di rete.

(*) 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 (GU L 333 del 27.12.2022, pag. 1).».

Articolo 4

Modifiche della direttiva 2013/36/UE

La direttiva 2013/36/UE è così modificata:

1) all'articolo 65, paragrafo 3, lettera a), il punto vi) è sostituito dal seguente:

«vi) terze parti cui le entità di cui ai punti da i) a iv) hanno esternalizzato funzioni o attività, compresi i fornitori terzi di servizi TIC di cui al capo V del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*);

(*) 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 (GU L 333 del 27.12.2022, pag. 1).;»

2) all'articolo 74, paragrafo 1, il primo comma è sostituito dal seguente:

«Gli enti sono dotati di solidi dispositivi di governance, ivi compresa una chiara struttura dell'organizzazione con linee di responsabilità ben definite, trasparenti e coerenti, di processi efficaci per l'identificazione, la gestione, la sorveglianza e la segnalazione dei rischi ai quali sono o potrebbero essere esposti, e di adeguati meccanismi di controllo interno, ivi compresi valide procedure amministrative e contabili, sistemi informatici e di rete istituiti e gestiti conformemente al regolamento (UE) 2022/2554 , nonché politiche e prassi di remunerazione che riflettano e promuovano una sana ed efficace gestione del rischio.»;

3) all'articolo 85, il paragrafo 2 è sostituito dal seguente:

«2. Le autorità competenti assicurano che gli enti dispongano di adeguati politiche e piani di emergenza e di continuità operativa, compresi le politiche e i piani di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC per la tecnologia che utilizzano per comunicare le informazioni e che tali piani siano istituiti, gestiti e testati a norma dell'articolo 11 del regolamento (UE) 2022/2554, affinché gli enti possano continuare a operare in caso di grave interruzione dell'operatività e limitare le perdite subite a seguito di tale interruzione.»;

4) all'articolo 97, paragrafo 1, è aggiunta la lettera seguente:

«d) i rischi evidenziati dalla verifica della resilienza operativa digitale conformemente al capo IV del regolamento (UE) 2022/2554;».

Articolo 5

Modifiche della direttiva 2014/59/UE

La direttiva 2014/59/UE è così modificata:

1) l'articolo 10 è così modificato:

a) al paragrafo 7, la lettera c) è sostituita dalla seguente:

«c) la dimostrazione di come le funzioni essenziali e le linee di business principali possano essere separate dalle altre funzioni, sul piano giuridico ed economico, nella misura necessaria, in modo da garantire la continuità e la resilienza operativa digitale in caso di dissesto dell'ente;»;

b) al paragrafo 7, la lettera q) è sostituita dalla seguente:

«q) una descrizione delle operazioni e dei sistemi essenziali per assicurare la continuità del funzionamento dei processi operativi dell'ente, compresi i sistemi informatici e di rete di cui al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*);

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

c) al paragrafo 9 è aggiunto il comma seguente:

«A norma dell'articolo 10 del regolamento (UE) n. 1093/2010, l'ABE rivede e, se del caso, aggiorna le norme tecniche di regolamentazione per tenere conto, tra l'altro, delle disposizioni del capo II del regolamento (UE) 2022/2554.»;

2) l'allegato è così modificato:

a) nella sezione A, il punto 16) è sostituito dal seguente:

«16) dispositivi e misure necessari per assicurare la continuità del funzionamento dei processi operativi dell'ente, compresi i sistemi informatici e di rete istituiti e gestiti a norma del regolamento (UE) 2022/2554;»;

b) la sezione B è modificata come segue:

i) il punto 14) è sostituito dal seguente:

«14) l'identificazione dei proprietari dei sistemi individuati al punto 13), i relativi accordi sul livello di servizio ed eventuali software e sistemi o licenze, compresa l'attribuzione alle persone giuridiche, operazioni essenziali e linee di business principali dell'ente, nonché un'identificazione dei fornitori terzi critici di servizi TIC definiti all'articolo 3, punto 23), del regolamento (UE) 2022/2554;»;

ii) è inserito il punto seguente:

«14 bis) i risultati delle prove di resilienza operativa digitale a norma del regolamento (UE) 2022/2554;»

c) la sezione C è modificata come segue:

i) il punto 4) è sostituito dal seguente:

«4) la misura in cui i contratti di servizio, compresi gli accordi contrattuali per l'utilizzo di servizi TIC, mantenuti dall'ente sono solidi e pienamente opponibili in caso di risoluzione dell'ente;»;

ii) è inserito il punto seguente:

«4 bis) la resilienza operativa digitale dei sistemi informatici e di rete che sostengono le funzioni essenziali e le linee di business principali dell'ente, tenendo conto delle segnalazioni di incidenti gravi connessi alle TIC e dei risultati delle prove di resilienza operativa digitale a norma del regolamento (UE) 2022/2554».

Articolo 6

Modifiche della direttiva 2014/65/UE

La direttiva 2014/65/UE è così modificata:

1) l'articolo 16 è così modificato:

a) il paragrafo 4 è sostituito dal seguente:

«4. Le imprese di investimento adottano misure ragionevoli per garantire la continuità e la regolarità nella prestazione di servizi e nell'esercizio di attività di investimento. A tal fine le imprese di investimento utilizzano sistemi appropriati e proporzionati, compresi sistemi di tecnologie dell'informazione e della comunicazione (TIC) istituiti e gestiti conformemente all'articolo 7 del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché risorse e procedure appropriate e proporzionate.

(*) 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 (GU L 333 del 27.12.2022, pag. 1).»;

b) al paragrafo 5, il secondo e il terzo comma sono sostituiti dal testo seguente:

«Le imprese di investimento dispongono di procedure amministrative e contabili sane, di meccanismi di controllo interno e di procedure efficaci per la valutazione del rischio.

Ferma restando la facoltà delle autorità competenti di ottenere accesso alle comunicazioni conformemente alla presente direttiva e al regolamento (UE) n. 600/2014, le imprese di investimento adottano efficaci meccanismi di sicurezza finalizzati a garantire, conformemente agli obblighi stabiliti da regolamento (UE) 2022/2554, la sicurezza e l'autenticazione dei mezzi per il trasferimento delle informazioni, a minimizzare i rischi di corruzione dei dati e di accesso non autorizzato e a prevenire la fuga di informazioni tutelando in ogni momento la riservatezza dei dati.»;

2) l'articolo 17 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Le imprese di investimento che effettuano negoziazione algoritmica pongono in essere controlli dei sistemi e del rischio efficaci e idonei per l'attività esercitata volti a garantire che i propri sistemi di negoziazione siano resilienti e dispongano di sufficiente capacità conformemente agli obblighi stabiliti al capo II del regolamento (UE) 2022/2554, siano soggetti a soglie e limiti di negoziazione appropriati e impediscano l'invio di ordini erronei o comunque un funzionamento dei sistemi tale da creare un mercato disordinato o contribuirvi.

Tali imprese pongono in essere anche controlli efficaci dei sistemi e del rischio per garantire che i sistemi di negoziazione non possano essere utilizzati per finalità contrarie al regolamento (UE) n. 596/2014 o alle regole di una sede di negoziazione a cui esse sono collegate.

Tali imprese di investimento dispongono di meccanismi efficaci di continuità operativa per rimediare a malfunzionamenti dei sistemi di negoziazione, compresi politica e piani di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti a norma dell'articolo 11 del regolamento (UE) 2022/2554 e provvedono affinché i loro sistemi siano verificati a fondo e soggetti a un monitoraggio adeguato per garantirne la conformità agli obblighi generali stabiliti nel presente paragrafo e agli obblighi specifici stabiliti ai capi II e IV del regolamento (UE) 2022/2554.»;

b) al paragrafo 7, la lettera a) è sostituita dalla seguente:

«a) precisare i requisiti organizzativi di cui ai paragrafi da 1 a 6, diversi da quelli connessi alla gestione dei rischi informatici, da imporre alle imprese di investimento che prestano diversi servizi di investimento, attività di investimento, servizi accessori o combinazioni degli stessi; le informazioni che precisano i requisiti organizzativi di cui al paragrafo 5 indicano i requisiti specifici per l'accesso diretto al mercato e per l'accesso sponsorizzato in modo tale da garantire che i controlli applicati all'accesso sponsorizzato siano almeno equivalenti a quelli applicati all'accesso diretto al mercato;»;

3) all'articolo 47, il paragrafo 1 è così modificato:

a) la lettera b) è sostituita dalla seguente:

«b) siano adeguatamente attrezzati per gestire i rischi ai quali sono esposti, compresi i rischi informatici ai sensi del capo II del regolamento (UE) 2022/2554, si dotino di dispositivi e sistemi adeguati per identificare i rischi che possano comprometterne il funzionamento e prendano misure efficaci per attenuare tali rischi;»;

b) la lettera c) è soppressa;

4) l'articolo 48 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Gli Stati membri garantiscono che i mercati regolamentati istituiscano e mantengano la loro resilienza operativa, conformemente agli obblighi stabiliti al capo II del regolamento (UE) 2022/2554, per garantire che i loro sistemi di negoziazione siano resilienti, abbiano capacità sufficiente per gestire i picchi di volume di ordini e messaggi, siano in grado di garantire negoziazioni ordinate in condizioni di mercato critiche, siano pienamente testati per garantire il rispetto di tali condizioni, siano soggetti a efficaci disposizioni in materia di continuità operativa, compresi politica e piani di continuità operativa delle TIC e piani di risposta e di ripristino relativi alle TIC istituiti ai sensi dell'articolo 11 del regolamento (UE) 2022/2554, per garantire la continuità dei servizi in caso di malfunzionamento dei loro sistemi di negoziazione.»;

b) il paragrafo 6 è sostituito dal seguente:

«6. Gli Stati membri si assicurano che i mercati regolamentati dispongano di sistemi, procedure e dispositivi efficaci, anche chiedendo ai membri o ai partecipanti di realizzare prove adeguate degli algoritmi e fornendo ambienti per facilitare la realizzazione di tali prove conformemente agli obblighi stabiliti ai capi II e IV del regolamento (UE) 2022/2554, per garantire che i sistemi algoritmici di negoziazione non possano creare o contribuire a creare condizioni di negoziazione anormali sul mercato e per gestire qualsiasi condizione di negoziazione anormale causata da tali sistemi algoritmici di negoziazione, tra cui sistemi per limitare il rapporto tra ordini non eseguiti e operazioni inserite nel sistema da un membro o partecipante, al fine di poter rallentare il flusso di ordini in caso di rischio che sia raggiunta la capacità del sistema e per limitare la dimensione minima dello scostamento di prezzo che può essere eseguita sul mercato e garantirne il rispetto.»;

c) il paragrafo 12 è così modificato:

i) la lettera a) è sostituita dalla seguente

«a) gli obblighi volti a garantire che i sistemi di negoziazione dei mercati regolamentati siano resilienti e abbiano una capacità adeguata, a eccezione degli obblighi relativi alla resilienza operativa digitale;»;

ii) la lettera g) è sostituita dalla seguente:

«g) gli obblighi volti a garantire una verifica adeguata degli algoritmi, diversa dalla verifica della resilienza operativa digitale, in modo da assicurare che i sistemi di negoziazione algoritmica, inclusi i sistemi di negoziazione algoritmica ad alta frequenza, non possano creare o contribuire a creare condizioni di negoziazione anormali sul mercato.».

Articolo 7

Modifiche della direttiva (UE) 2015/2366

La direttiva (UE) 2015/2366 è così modificata:

1) all'articolo 3, la lettera j) è sostituita dalla seguente:

«j) ai servizi forniti da prestatori di servizi tecnici, che supportano la prestazione dei servizi di pagamento, senza mai entrare in possesso dei fondi da trasferire, compresi l'elaborazione e la registrazione di dati, i servizi fiduciari e di protezione della riservatezza, l'autenticazione dei dati e delle entità, la fornitura di reti di tecnologie dell'informazione e della comunicazione (*information and communication technology* – TIC) e di comunicazione, la fornitura e la manutenzione di terminali e dispositivi utilizzati per i servizi di pagamento a esclusione dei servizi di disposizione di ordine di pagamento e dei servizi di informazione sui conti;»;

2) all'articolo 5, il paragrafo 1 è così modificato:

a) il primo comma è così modificato:

i) la lettera e) è sostituita dalla seguente:

«e) una descrizione dei dispositivi di governo societario e dei meccanismi di controllo interno, ivi comprese le procedure amministrative, di gestione del rischio e contabili, del richiedente, nonché gli accordi per l'utilizzo di servizi di TIC a noma del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), che dimostri che tali dispositivi di governo societario e meccanismi di controllo interno siano proporzionati, appropriati, validi e adeguati;

(*) 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 (GU L 333 del 27.12.2022, pag. 1).";

ii) la lettera f) è sostituita dalla seguente:

«f) una descrizione della procedura esistente per monitorare e gestire gli incidenti relativi alla sicurezza e i reclami dei clienti in materia di sicurezza e per darvi seguito, compreso un meccanismo di notifica degli incidenti che tenga conto degli obblighi di notifica dell'istituto di pagamento di cui al capo III del regolamento (UE) 2022/2554»

iii) la lettera h) è sostituita dalla seguente:

«h) una descrizione delle disposizioni in materia di continuità operativa, tra cui l'individuazione chiara delle operazioni critiche, politica e piani di continuità operativa delle TIC e piani di risposta e di ripristino relativi alle TIC efficaci nonché una procedura per testare periodicamente e riesaminare l'adeguatezza e l'efficacia di tali piani a norma del regolamento (UE) 2022/2554;»;

b) il terzo comma è sostituito dal seguente:

«Le misure di controllo e di mitigazione in materia di sicurezza di cui al primo comma, lettera j), indicano in che modo garantiscono un elevato livello di resilienza operativa digitale conformemente al capo II del regolamento (UE) 2022/2554, in particolare, in relazione alla sicurezza tecnica e protezione dei dati, anche per il software e i sistemi TIC utilizzati dal richiedente o dalle imprese alle quali questi esternalizza la totalità o parte delle sue attività. Tali misure comprendono anche le misure di sicurezza di cui all'articolo 95, paragrafo 1, della presente direttiva. Tali misure tengono conto degli orientamenti dell'ABE relativi alle misure di sicurezza di cui all'articolo 95, paragrafo 3, della presente direttiva una volta emanati.»;

3) all'articolo 19, paragrafo 6, il secondo comma è sostituito dal seguente:

«L'esternalizzazione di funzioni operative importanti, tra cui i sistemi TIC, non deve mettere materialmente a repentaglio la qualità del controllo interno dell'istituto di pagamento né la capacità delle autorità competenti di controllare e documentare che l'istituto di pagamento adempia a tutti gli obblighi definiti dalla presente direttiva.»;

4) all'articolo 95, paragrafo 1, è aggiunto il comma seguente:

«Il primo comma lascia impregiudicata l'applicazione del capo II del regolamento (UE) 2022/2554:

a) ai prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere a), b) e d), della presente direttiva;

b) ai prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della presente direttiva;

c) agli istituti di pagamento esentati a norma dell'articolo 32, paragrafo 1, della presente direttiva; e

d) agli istituti di moneta elettronica che beneficiano di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE.»;

5) all'articolo 96 è aggiunto il paragrafo seguente:

«7. Gli Stati membri assicurano che i paragrafi da 1 a 5 del presente articolo non si applichino:

a) ai prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere a), b) e d), della presente direttiva;

b) ai prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della presente direttiva;

c) agli istituti di pagamento esentati a norma dell'articolo 32, paragrafo 1, della presente direttiva; e

d) agli istituti di moneta elettronica che beneficiano di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE.»;

6) all'articolo 98, il paragrafo 5 è sostituito dal seguente:

«5. A norma dell'articolo 10 del regolamento (UE) n. 1093/2010, l'ABE periodicamente rivede e, se del caso, aggiorna le norme tecniche di regolamentazione, tra l'altro, per tenere conto dell'innovazione e dei progressi tecnologici, nonché delle disposizioni del capo II del regolamento (UE) 2022/2554».

Articolo 8

Modifica della direttiva (UE) 2016/2341

All'articolo 21 della direttiva (UE) 2016/2341, il paragrafo 5 è sostituito dal seguente:

«5. Gli Stati membri assicurano che gli EPAP adottino misure ragionevoli atte a garantire la continuità e la regolarità dello svolgimento delle loro attività, tra cui l'elaborazione di piani di emergenza. A tal fine gli EPAP utilizzano sistemi,

risorse e procedure adeguati e proporzionati e, in particolare, istituiscono e gestiscono sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), ove applicabile.

(*) 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 (GU L 333 del 27.12.2022, pag. 1).».

Articolo 9

Recepimento

1. Entro il 17 gennaio 2025, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione.

Essi applicano tali misure a decorrere dal 17 gennaio 2025.

Le misure adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni principali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 10

Entrata in vigore

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

Articolo 11

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK

DIRETTIVA (UE) 2022/2557 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) In quanto fornitori di servizi essenziali, i soggetti critici svolgono un ruolo indispensabile per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno in un'economia dell'Unione sempre più interdipendente. È pertanto essenziale definire un quadro a livello dell'Unione volto sia a rafforzare la resilienza dei soggetti critici nel mercato interno, stabilendo norme minime armonizzate, sia ad assistere tali soggetti mediante misure di sostegno e vigilanza coerenti e dedicate.

(2) La direttiva 2008/114/CE del Consiglio ([4]) stabilisce una procedura di designazione delle infrastrutture critiche europee nei settori dell'energia e dei trasporti, il cui danneggiamento o la cui distruzione avrebbe un significativo impatto transfrontaliero su almeno due Stati membri. Tale direttiva si incentra esclusivamente sulla protezione di tali infrastrutture. La valutazione di tale direttiva, svolta nel 2019, ha riscontrato tuttavia che, dato il carattere sempre più interconnesso e transfrontaliero delle operazioni effettuate utilizzando infrastrutture critiche, le misure di protezione riguardanti solo singole strutture non sono sufficienti per evitare il verificarsi di perturbazioni. È quindi necessario modificare l'approccio applicato per garantire che si tenga maggiormente conto dei rischi, che il ruolo e i compiti dei soggetti critici quali fornitori di servizi essenziali per il funzionamento del mercato interno

([1]) GU C 286 del 16.7.2021, pag. 170.
([2]) GU C 440 del 29.10.2021, pag. 99.
([3]) Posizione del Parlamento europeo del 22 novembre 2022 (non ancora pubblicata nella Gazzetta Ufficiale) e decisione del Consiglio dell'8 dicembre 2022.
([4]) Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008, pag. 75).

siano meglio definiti e coerenti, e che siano adottate norme a livello dell'Unione per rafforzare la resilienza di tali soggetti. I soggetti critici dovrebbero essere in grado di rafforzare la loro capacità di prevenire, proteggere, rispondere, resistere, mitigare, assorbire, adattarsi e ripristinare le proprie capacità operative a seguito di incidenti che possono perturbare la fornitura di servizi essenziali.

(3) Sebbene una serie di misure esistenti a livello dell'Unione, quali il Programma europeo per la protezione delle infrastrutture critiche, e a livello nazionale miri a sostenere la protezione delle infrastrutture critiche nell'Unione, si dovrebbe fare di più affinché i soggetti che gestiscono tali infrastrutture siano meglio preparati ad affrontare i rischi per la loro operatività, che potrebbero portare alla perturbazione della fornitura di servizi essenziali. Si dovrebbe fare di più affinché i soggetti che gestiscono tali infrastrutture siano meglio preparati a un panorama delle sfide dinamico, che comprende minacce ibride e terroristiche in evoluzione e crescenti interdipendenze fra infrastruttura e settori. Inoltre, vi è un aumento del rischio fisico dovuto alle catastrofi naturali e ai cambiamenti climatici, che intensifica la frequenza e la portata degli eventi meteorologici estremi e comporta cambiamenti a lungo termine delle condizioni climatiche medie che possono ridurre la capacità, l'efficienza e la durata operativa di alcuni tipi di infrastrutture se non sono in atto misure di adattamento ai cambiamenti climatici. Inoltre, il mercato interno è caratterizzato da una frammentazione per quanto riguarda l'individuazione dei soggetti critici, in quanto i settori e le categorie di soggetti rilevanti non sono riconosciuti come critici in modo coerente in tutti gli Stati membri. La presente direttiva dovrebbe pertanto raggiungere un solido livello di armonizzazione in termini di settori e categorie di soggetti che rientrano nel suo ambito di applicazione.

(4) Determinati settori dell'economia, come l'energia e i trasporti, sono già regolamentati da atti giuridici settoriali dell'Unione, ma tali atti giuridici dell'Unione disciplinano unicamente determinati aspetti della resilienza dei soggetti che operano nell'ambito di tali settori. Per affrontare in modo globale la resilienza dei soggetti critici ai fini del corretto funzionamento del mercato interno, la presente direttiva crea un quadro generale per affrontare la resilienza dei soggetti critici rispetto a tutti i rischi, naturali e di origine umana, accidentali e intenzionali.

(5) Le crescenti interdipendenze tra infrastruttura e settori sono il risultato di una rete di fornitura di servizi sempre più transfrontaliera e interconnessa, che utilizza infrastrutture essenziali in tutta l'Unione nei settori dell'energia, dei trasporti, bancario, delle acque potabili, delle acque reflue, della produzione, trasformazione e distribuzione di alimenti, della sanità, dello spazio, delle infrastrutture dei mercati finanziari e delle infrastrutture digitali, e di determinati aspetti della pubblica amministrazione. Il settore spaziale rientra nell'ambito di applicazione della presente direttiva per quanto riguarda la fornitura di determinati servizi che dipendono da infrastrutture di terra possedute, gestite e utilizzate dagli Stati membri o da soggetti privati, pertanto le infrastrutture possedute, gestite o utilizzate dall'Unione o per suo conto nell'ambito del suo programma spaziale non rientrano nell'ambito di applicazione della presente direttiva.

In riferimento al settore energetico e, in particolare, ai metodi di produzione e trasmissione di energia elettrica (per quanto riguarda la fornitura di energia elettrica), è inteso che, se ritenuto opportuno, la produzione di energia elettrica può includere le componenti delle centrali nucleari destinate alla trasmissione di energia elettrica ma non gli elementi specificamente nucleari disciplinati da trattati e dal diritto dell'Unione, compresi i pertinenti atti giuridici dell'Unione relativi all'energia nucleare. Il processo di identificazione dei soggetti critici nel settore alimentare dovrebbe rispecchiare adeguatamente la natura del mercato interno in tale settore e le disposizioni di dettaglio dell'Unione relative ai principi e ai requisiti generali della normativa alimentare e della sicurezza alimentare. Pertanto, al fine di assicurare che vi sia un approccio proporzionato e rispecchiare adeguatamente il ruolo e l'importanza di tali soggetti a livello nazionale, tali soggetti critici dovrebbero essere identificati solo tra le imprese alimentari, con o senza scopo di lucro, pubbliche o private, che operano esclusivamente nella logistica e nella distribuzione all'ingrosso nonché nella produzione e trasformazione industriale su larga scala e che detengono una quota di mercato significativa a livello nazionale. Tali interdipendenze implicano che qualsiasi perturbazione di servizi essenziali, anche se inizialmente limitata a un soggetto o a un settore, possa avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e a lungo termine sulla fornitura di servizi in tutto il mercato interno. Gravi crisi, come la pandemia di COVID-19, hanno mostrato la vulnerabilità delle nostre società sempre più interdipendenti di fronte a rischi di bassa probabilità e impatto elevato.

(6) I soggetti che intervengono nella fornitura di servizi essenziali devono sempre più spesso rispettare requisiti divergenti imposti dal diritto nazionale. Il fatto che alcuni Stati membri prevedano per tali soggetti requisiti di sicurezza meno rigorosi non solo determina diversi livelli di resilienza, ma rischia anche di incidere negativamente sul mantenimento di funzioni vitali della società o di attività economiche nell'Unione e crea altresì ostacoli al corretto funzionamento del mercato interno. Gli investitori e le imprese possono fare affidamento su soggetti critici che sono resilienti e confidare in essi, in quanto l'affidabilità e la fiducia sono pietre angolari di un mercato interno ben funzionante. Tipi di soggetti simili sono considerati critici da alcuni Stati membri ma non da altri, e quelli individuati come critici devono soddisfare requisiti divergenti nei vari Stati membri. Ciò crea oneri amministrativi supplementari e non necessari per le imprese che operano a livello transfrontaliero, in particolare per quelle attive negli Stati membri con requisiti più rigorosi. Un quadro a livello di Unione determinerebbe quindi anche la creazione di condizioni di parità per i soggetti critici in tutta l'Unione.

(7) È necessario stabilire norme minime armonizzate per garantire la fornitura di servizi essenziali nel mercato interno, aumentare la resilienza dei soggetti critici e migliorare la cooperazione transfrontaliera tra le autorità competenti. È importante che tali norme siano adeguate alle esigenze future in termini di concezione e attuazione, consentendo al contempo la necessaria flessibilità. È altresì fondamentale migliorare la capacità dei soggetti critici di fornire servizi essenziali di fronte a una serie diversificata di rischi.

(8) Per conseguire un livello elevato di resilienza, gli Stati membri dovrebbero individuare i soggetti critici che saranno tenuti a soddisfare specifici requisiti, che saranno oggetto di vigilanza e che riceveranno anche particolare sostegno e orientamento rispetto a tutti i rischi rilevanti.

(9) Data l'importanza della cibersicurezza per la resilienza dei soggetti critici e a fini di congruenza, dovrebbe essere assicurato, ogniqualvolta possibile, un approccio coerente fra la presente direttiva e la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([5]). Alla luce della maggiore frequenza e delle particolari caratteristiche dei rischi informatici, la direttiva (UE) 2022/2555 impone a un'ampia gamma di soggetti requisiti dettagliati per garantire la propria cibersicurezza. Dato che l'aspetto della cibersicurezza è trattato in modo sufficiente da tale direttiva (UE) 2022/2555, le materie da essa disciplinate dovrebbero essere escluse dall'ambito di applicazione della presente direttiva, fermo restando il particolare regime per i soggetti del settore delle infrastrutture digitali.

(10) Qualora le disposizioni di atti giuridici settoriali dell'Unione impongano ai soggetti critici di adottare misure per rafforzare la propria resilienza o di notificare gli incidenti, e qualora tali requisiti siano riconosciuti dagli Stati membri come almeno equivalenti ai corrispondenti obblighi stabiliti dalla presente direttiva, le pertinenti disposizioni della presente direttiva non dovrebbero applicarsi, in modo da evitare duplicazioni e oneri non necessari. In tal caso dovrebbero applicarsi le pertinenti disposizioni di tali atti giuridici dell'Unione. Qualora non si applichino le pertinenti disposizioni della presente direttiva, non dovrebbero applicarsi nemmeno le disposizioni di cui alla presente direttiva in materia di vigilanza ed esecuzione.

(11) La presente direttiva non incide sulle competenze degli Stati membri e delle loro autorità in termini di autonomia amministrativa né sulla loro responsabilità di salvaguardare la sicurezza nazionale e la difesa o il loro potere di salvaguardare altre funzioni essenziali dello Stato, in particolare per quanto riguarda la pubblica sicurezza, l'integrità territoriale e il mantenimento dell'ordine pubblico. L'esclusione degli enti della pubblica amministrazione dall'ambito di applicazione della presente direttiva dovrebbe applicarsi a enti le cui attività sono svolte principalmente nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati. Tuttavia gli enti della pubblica amministrazione le cui attività sono connesse solo marginalmente a tali settori dovrebbero continuare a rientrare nell'ambito di applicazione della presente direttiva. Ai fini della presente direttiva, i soggetti con competenze normative non sono considerati quali operanti nel settore dell'attività di contrasto e non sono pertanto esclusi per tali motivi dall'ambito di applicazione della presente direttiva. Gli enti della pubblica amministrazione istituiti congiuntamente con un paese terzo in virtù di un accordo internazionale sono esclusi dall'ambito di applicazione della presente direttiva. La presente direttiva non si applica alle missioni diplomatiche e consolari degli Stati membri nei paesi terzi.

([5]) 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, che modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (cfr. pagina 80 della presente Gazzetta ufficiale).

Taluni soggetti critici operano nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati, o forniscono servizi esclusivamente agli enti della pubblica amministrazione che operano principalmente in tali settori. Tenuto conto della responsabilità degli Stati membri di salvaguardare la sicurezza nazionale e la difesa, gli Stati membri dovrebbero poter decidere che gli obblighi stabiliti dalla presente direttiva ai soggetti critici non si applichino in tutto o in parte a tali soggetti critici se i servizi che forniscono o le attività che svolgono sono legati principalmente ai settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati. I soggetti critici le cui attività sono connesse solo marginalmente a tali settori dovrebbero continuare a rientrare nell'ambito di applicazione della presente direttiva. Nessuno Stato membro dovrebbe essere tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria sicurezza nazionale. Sono pertinenti le norme dell'Unione o nazionali per la protezione delle informazioni classificate e gli accordi di riservatezza.

(12) Al fine di non compromettere la sicurezza nazionale o la sicurezza e gli interessi commerciali dei soggetti critici, l'accesso alle informazioni sensibili nonché il loro scambio e trattamento dovrebbero essere effettuati in modo prudente, con particolare attenzione ai canali di trasmissione e alle capacità di archiviazione utilizzate.

(13) Per garantire un approccio globale alla resilienza dei soggetti critici, ciascuno Stato membro dovrebbe disporre di una strategia per rafforzare la resilienza dei soggetti critici («strategia»). La strategia dovrebbe stabilire le misure e gli obiettivi strategici da attuare. Ai fini di una maggiore coerenza ed efficienza, la strategia dovrebbe essere concepita in modo da integrare senza soluzione di continuità le politiche esistenti basandosi, ove possibile, su pertinenti strategie a livello nazionale e settoriale, piani o documenti analoghi esistenti. Ai fini della realizzazione di un approccio globale, gli Stati membri dovrebbero provvedere affinché le loro strategie prevedano un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e le autorità competenti a norma della direttiva (UE) 2022/2555 nel contesto della condivisione delle informazioni sui rischi di cibersicurezza, sulle minacce e sugli incidenti informatici e sui rischi, minacce e incidenti non informatici e nel contesto dello svolgimento di compiti di vigilanza. Nell'attuare le proprie strategie, gli Stati membri dovrebbero tenere debitamente conto della natura ibrida delle minacce ai soggetti critici.

(14) Gli Stati membri dovrebbero comunicare alla Commissione le loro strategie e i relativi aggiornamenti sostanziali, in particolare al fine di consentire alla Commissione di valutare la corretta applicazione della presente direttiva per quanto riguarda gli approcci strategici in materia di resilienza dei soggetti critici a livello nazionale. Se necessario, le strategie potrebbero essere comunicate sotto forma di informazioni classificate. La Commissione dovrebbe elaborare una relazione di sintesi delle strategie comunicate dagli Stati membri che funga da base per gli scambi al fine di individuare le migliori prassi e le questioni di interesse comune nel quadro del gruppo per la resilienza dei soggetti critici. Data la natura sensibile delle informazioni aggregate incluse nella relazione di sintesi, siano esse classificate o meno, la Commissione dovrebbe gestire tale relazione di sintesi con un adeguato livello di consapevolezza riguardo alla sicurezza dei soggetti critici, degli Stati membri e dell'Unione. La relazione di sintesi e le strategie dovrebbero essere salvaguardate contro azioni illecite o dolose e dovrebbero essere accessibili solo alle persone autorizzate al fine di conseguire gli obiettivi della presente direttiva. La comunicazione delle strategie e dei loro aggiornamenti sostanziali dovrebbe inoltre servire ad aiutare la Commissione a comprendere gli sviluppi negli approcci alla resilienza dei soggetti critici e contribuire al monitoraggio dell'impatto e del valore aggiunto della presente direttiva, che la Commissione è tenuta a riesaminare periodicamente.

(15) Le azioni degli Stati membri per individuare i soggetti critici e contribuire a garantirne la resilienza dovrebbero seguire un approccio basato sui rischi incentrato sui soggetti maggiormente rilevanti per lo svolgimento di funzioni vitali della società o di attività economiche. Per garantire un tale approccio mirato, ciascuno Stato membro dovrebbe effettuare, in un quadro armonizzato, una valutazione dei rischi rilevanti, naturali e di origine umana, compresi quelli di natura intersettoriale o transfrontaliera, che potrebbero ripercuotersi negativamente sulla fornitura di servizi essenziali, compresi gli incidenti, le catastrofi naturali, le emergenze di sanità pubblica come le pandemie e le minacce ibride o altre minacce antagoniste, inclusi i reati di terrorismo, le infiltrazioni criminali e il sabotaggio («valutazione del rischio dello Stato membro»). Nell'effettuare tali valutazioni del rischio dello Stato membro, gli Stati membri dovrebbero tenere conto di altre valutazioni del rischio generali o settoriali svolte ai sensi di altri atti giuridici dell'Unione, e dovrebbero prendere in considerazione la misura in cui i settori dipendono l'uno dall'altro, compresi i settori di altri Stati membri e di paesi terzi. I risultati della valutazione del rischio dello Stato membro dovrebbero essere utilizzati ai fini dell'individuazione dei soggetti critici e di aiutare tali soggetti a conformarsi ai

rispettivi obblighi in materia di resilienza. La presente direttiva si applica solo agli Stati membri e ai soggetti critici che operano all'interno dell'Unione. Tuttavia, le competenze e le conoscenze generate dalle autorità competenti, in particolare attraverso le valutazioni del rischio, e dalla Commissione, in particolare attraverso varie forme di sostegno e cooperazione, potrebbero essere utilizzate, se del caso e conformemente agli strumenti giuridici applicabili, a beneficio dei paesi terzi, in particolare quelli situati nell'immediato vicinato dell'Unione, alimentando la cooperazione esistente in materia di resilienza.

(16) Per garantire che tutti i soggetti rilevanti siano soggetti alle prescrizioni in materia di resilienza della presente direttiva e per ridurre le divergenze a tale riguardo, è importante stabilire norme armonizzate che consentano un'individuazione coerente dei soggetti critici in tutta l'Unione, consentendo al tempo stesso agli Stati membri di riflettere adeguatamente il ruolo e l'importanza di tali soggetti a livello nazionale. Nell'applicare i criteri stabiliti nella presente direttiva, ciascun Stato membro dovrebbe individuare i soggetti che forniscono uno o più servizi essenziali e che gestiscono e dispongono di infrastrutture critiche situate nel proprio territorio. Si dovrebbe ritenere che un soggetto operi nel territorio di uno Stato membro in cui svolge le attività necessarie per il servizio o i servizi essenziali in questione e in cui è ubicata l'infrastruttura critica di detto soggetto utilizzata per fornire tale servizio o tali servizi. Qualora in uno Stato membro non esista un soggetto che soddisfi tali criteri, tale Stato membro non dovrebbe avere l'obbligo di individuare un soggetto critico nel settore o sottosettore corrispondente. Ai fini di efficacia, efficienza, coerenza e certezza del diritto, dovrebbero essere stabilite norme adeguate in materia di notifica ai soggetti individuati come critici.

(17) Gli Stati membri dovrebbero trasmettere alla Commissione, in modo da conseguire gli obiettivi della presente direttiva, un elenco dei servizi essenziali, il numero di soggetti critici individuati per ciascuno dei settori e sottosettori di cui all'allegato e per il servizio o i servizi essenziali che ogni soggetto fornisce e, se applicate, le soglie. Dovrebbe essere possibile presentare le soglie come tali o in forma aggregata, il che significa che le informazioni possono essere comunicate nei valori medi per area geografica, per anno, per settore, per sottosettore, o con altri mezzi, e possono includere informazioni sulla gamma degli indicatori forniti.

(18) Dovrebbero essere stabiliti criteri per determinare la rilevanza degli effetti negativi prodotti da un incidente. Tali criteri dovrebbero basarsi su quelli di cui alla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([6]) per sfruttare al meglio gli sforzi compiuti dagli Stati membri per individuare gli operatori dei servizi essenziali di cui a tale direttiva e per trarre insegnamento dall'esperienza acquisita in materia. Gravi crisi, come la pandemia di COVID-19, hanno dimostrato l'importanza di garantire la sicurezza della catena di approvvigionamento e come la sua perturbazione possa avere ripercussioni economiche e sociali negative in un gran numero di settori e a livello transfrontaliero. Pertanto, nel determinare la misura in cui altri settori e sottosettori dipendono dai servizi essenziali forniti da un soggetto critico, gli Stati membri dovrebbero tenere conto, per quanto possibile, anche degli effetti sulla catena di approvvigionamento.

(19) Conformemente al diritto dell'Unione e nazionale applicabile, compreso il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio ([7]) che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, occorre prendere atto della potenziale minaccia rappresentata dalla proprietà estera di infrastrutture critiche all'interno dell'Unione, poiché dal corretto funzionamento delle infrastrutture critiche dipendono i servizi, l'economia, la libera circolazione e la sicurezza dei cittadini dell'Unione.

(20) La direttiva (UE) 2022/2555 impone ai soggetti che appartengono al settore delle infrastrutture digitali, che potrebbero essere considerati soggetti critici ai sensi della presente direttiva, di adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete e per notificare incidenti e minacce informatiche significativi. Poiché le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, la direttiva (UE) 2022/2555 applica un approccio «multirischio» che comprende la resilienza dei sistemi informatici e di rete nonché dei componenti e ambienti fisici di tali sistemi.

([6]) 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).

([7]) Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione (GU L 79I del 21.3.2019, pag. 1).

Dato che le prescrizioni previste dalla direttiva (UE) 2022/2555 a tale riguardo sono almeno equivalenti ai corrispondenti obblighi previsti dalla presente direttiva, gli obblighi previsti dall'articolo 11 e dai capi III, IV e VI della presente direttiva non dovrebbero applicarsi ai soggetti che appartengono al settore delle infrastrutture digitali al fine di evitare duplicazioni e oneri amministrativi non necessari. Tuttavia, considerata l'importanza dei servizi forniti dai soggetti che appartengono al settore delle infrastrutture digitali ai soggetti critici appartenenti a tutti gli altri settori, gli Stati membri dovrebbero individuare quali critici, in base ai criteri previsti dalla presente direttiva e ricorrendo alla procedura ivi stabilita, i soggetti che appartengono al settore delle infrastrutture digitali. Di conseguenza, dovrebbero applicarsi le strategie, le valutazioni del rischio dello Stato membro e le misure di sostegno di cui al capo II della presente direttiva. Gli Stati membri dovrebbero poter adottare o mantenere in vigore disposizioni di diritto interno atte a conseguire un livello di resilienza più elevato per tali soggetti critici, a condizione che dette disposizioni siano coerenti con il diritto dell'Unione applicabile.

(21) Il diritto dell'Unione in materia di servizi finanziari stabilisce per i soggetti finanziari requisiti dettagliati di gestione di tutti i rischi cui sono esposti, compresi i rischi operativi, e di garanzia di continuità operativa. Tale diritto include i regolamenti (UE) n. 648/2012 ([8]), (UE) n. 575/2013 ([9]) e (UE) n. 600/2014 ([10]) del Parlamento europeo e del Consiglio e le direttive 2013/36/UE ([11]) e 2014/65/UE ([12]) del Parlamento europeo e del Consiglio. Tale quadro giuridico è integrato dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([13]), che stabilisce gli obblighi applicabili ai soggetti finanziari per la gestione dei rischi informatici, anche per quanto riguarda la protezione delle infrastrutture delle tecnologie dell'informazione e della comunicazione fisiche. Dato che la resilienza di tali soggetti è pertanto esaurientemente disciplinata, l'articolo 11 e i capi III, IV e VI della presente direttiva non dovrebbero applicarsi a tali soggetti, al fine di evitare duplicazioni e oneri amministrativi non necessari.

Tuttavia, considerata l'importanza dei servizi forniti dai soggetti del settore finanziario ai soggetti critici appartenenti a tutti gli altri settori, gli Stati membri dovrebbero individuare quali soggetti critici, in base ai criteri previsti dalla presente direttiva e ricorrendo alla procedura ivi stabilita, i soggetti del settore finanziario. Di conseguenza, dovrebbero applicarsi le strategie, le valutazioni del rischio dello Stato membro e le misure di sostegno di cui al capo II della presente direttiva. Gli Stati membri dovrebbero poter adottare o mantenere in vigore disposizioni di diritto interno atte a conseguire un livello di resilienza più elevato per tali soggetti critici, a condizione che tali disposizioni siano coerenti con il diritto dell'Unione applicabile.

(22) Gli Stati membri dovrebbero designare o istituire le autorità competenti a vigilare sull'applicazione delle norme della presente direttiva e, ove necessario, a farle rispettare, e dovrebbero provvedere affinché tali autorità dispongano di poteri e risorse adeguate. Alla luce delle differenze esistenti tra le strutture amministrative nazionali, al fine di salvaguardare gli accordi settoriali esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione, e al fine di evitare duplicazioni, è opportuno che gli Stati membri abbiano la facoltà di designare o istituire più di un'autorità nazionale competente. Qualora gli Stati membri designino o istituiscano più di un'autorità competente dovrebbero delineare chiaramente i rispettivi compiti delle autorità interessate e garantire fra di esse una cooperazione agevole ed efficace. Tutte le autorità competenti dovrebbero inoltre cooperare in modo più generale con le altre autorità rilevanti, sia a livello dell'Unione sia a livello nazionale.

([8]) 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).

([9]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).

([10]) Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84).

([11]) 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 e sulle imprese di investimento, 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).

([12]) 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).

([13]) 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 (cfr. pagina 1 della presente Gazzetta ufficiale).

(23) Al fine di agevolare la cooperazione e la comunicazione transfrontaliere e per consentire l'efficace attuazione della presente direttiva, ogni Stato membro dovrebbe, ferme restando le prescrizioni degli atti giuridici settoriali dell'Unione, designare un punto di contatto unico incaricato di coordinare le questioni relative alla resilienza dei soggetti critici e la cooperazione transfrontaliera a livello dell'Unione («punto di contatto unico»), ove opportuno all'interno di un'autorità competente. Ciascun punto di contatto unico dovrebbe fungere da collegamento e coordinare le comunicazioni, ove opportuno, con le autorità competenti del proprio Stato membro, con i punti di contatto unici degli altri Stati membri e con il gruppo per la resilienza dei soggetti critici.

(24) Le autorità competenti ai sensi della presente direttiva e le autorità competenti ai sensi della direttiva (UE) 2022/2555 dovrebbero cooperare e scambiarsi informazioni in relazione ai rischi di cibersicurezza, alle minacce e agli incidenti informatici nonché ai rischi, alle minacce e agli incidenti non informatici che hanno ripercussioni sui soggetti critici, così come in relazione alle misure pertinenti adottate dalle autorità competenti ai sensi della presente direttiva e dalle autorità competenti ai sensi della direttiva (UE) 2022/2555 È importante che gli Stati membri provvedano affinché le prescrizioni di cui alla presente direttiva e di cui alla direttiva (UE) 2022/2555 siano attuate in modo complementare e che sui soggetti critici non gravi un onere amministrativo superiore a quanto necessario per conseguire gli obiettivi della presente direttiva e di tale direttiva.

(25) Gli Stati membri dovrebbero sostenere i soggetti critici, compresi quelli che si qualificano come piccole e medie imprese, nel rafforzamento della loro resilienza, nel rispetto degli obblighi degli Stati membri stabiliti dalla presente direttiva, ferma restando la responsabilità giuridica dei soggetti critici stessi quanto al garantire tale ottemperanza, e nel farlo dovrebbero evitare oneri amministrativi eccessivi. Gli Stati membri potrebbero in particolare sviluppare materiali e metodologie di orientamento, contribuire all'organizzazione di esercitazioni per testare la resilienza dei soggetti critici e fornire consulenza e corsi di formazione per il personale dei soggetti critici. Ove necessario e giustificato da obiettivi di interesse pubblico, gli Stati membri potrebbero fornire risorse finanziarie e dovrebbero agevolare la condivisione volontaria di informazioni e lo scambio di buone prassi fra soggetti critici, ferma restando l'applicazione delle norme in materia di concorrenza stabilite nel trattato sul funzionamento dell'Unione europea (TFUE).

(26) Al fine di rafforzare la resilienza dei soggetti critici individuati dagli Stati membri e di ridurre gli oneri amministrativi per tali soggetti critici, le autorità competenti dovrebbero consultarsi ogniqualvolta sia opportuno al fine di garantire un'applicazione coerente della presente direttiva. Tali consultazioni dovrebbero essere avviate su richiesta di qualsiasi autorità competente interessata e dovrebbero incentrarsi sulla garanzia di un approccio convergente nei confronti di soggetti critici interconnessi che utilizzano infrastrutture critiche fisicamente collegate tra due o più Stati membri, che appartengono agli stessi gruppi o strutture societarie o che sono stati individuati in uno Stato membro e forniscono servizi essenziali ad altri Stati membri o in altri Stati membri.

(27) Qualora le disposizioni del diritto dell'Unione o nazionale richiedano ai soggetti critici di valutare i rischi rilevanti ai fini della presente direttiva e di adottare misure per garantire la propria resilienza, tali obblighi dovrebbero essere adeguatamente presi in considerazione ai fini della vigilanza sul rispetto della presente direttiva da parte dei soggetti critici.

(28) I soggetti critici dovrebbero avere una conoscenza esaustiva dei rischi rilevanti a cui sono esposti e il dovere di analizzarli. A tal fine, dovrebbero effettuare valutazioni del rischio ogniqualvolta necessario date le loro specifiche circostanze e l'evolversi di tali rischi, e in ogni caso ogni quattro anni, al fine di valutare tutti i rischi rilevanti che potrebbero perturbare in modo significativo la fornitura dei loro servizi essenziali («valutazione del rischio dei soggetti critici»). Qualora i soggetti critici abbiano effettuato altre valutazioni del rischio o redatto documenti conformemente agli obblighi previsti da altri atti giuridici pertinenti per la loro valutazione del rischio dei soggetti critici, essi dovrebbero poter utilizzare tali valutazioni e documenti per soddisfare i requisiti di cui alla presente direttiva che riguardano le valutazioni del rischio dei soggetti critici. Un'autorità competente dovrebbe poter dichiarare che una valutazione del rischio esistente effettuata da un soggetto critico che affronta i rischi rilevanti e il relativo grado di dipendenza, è conforme, in tutto o in parte, agli obblighi previsti dalla presente direttiva.

(29) I soggetti critici dovrebbero adottare misure tecniche, di sicurezza e organizzative adeguate e proporzionate ai rischi cui sono esposti, allo scopo di prevenire gli incidenti, di proteggersi da essi, di darvi risposta, di resistervi, di mitigarli, assorbirli, di adattarvisi e di ripristinare le proprie capacità operative. I soggetti critici dovrebbero adottare tali misure in conformità della presente direttiva, ma i dettagli e la portata di tali misure dovrebbero rispecchiare in modo adeguato e proporzionato i vari rischi che ciascun soggetto critico ha identificato nell'ambito della sua valutazione del rischio del soggetto critico e le specificità del soggetto stesso. Per promuovere un approccio coerente a livello di Unione, la Commissione dovrebbe, previa consultazione del gruppo per la resilienza dei soggetti critici, adottare linee guida non vincolanti per specificare ulteriormente tali misure tecniche, di sicurezza e organizzative. Gli Stati membri dovrebbero provvedere affinché ciascun soggetto critico designi un funzionario di collegamento o equivalente come punto di contatto con le autorità competenti.

(30) A fini di efficacia e di responsabilizzazione, i soggetti critici dovrebbero descrivere le misure da essi adottate con un livello di dettaglio che consegua sufficientemente gli obiettivi di efficacia e di responsabilizzazione stabiliti, tenuto conto dei rischi individuati, in un piano di resilienza o in uno o più documenti equivalenti a un piano di resilienza, e dovrebbero mettere in pratica tale piano. Qualora un soggetto critico abbia già adottato misure tecniche, di sicurezza e organizzative e redatto documenti conformemente ad altri atti giuridici pertinenti per le misure di rafforzamento della resilienza ai sensi della presente direttiva, esso dovrebbe poter utilizzare tali misure e documenti per soddisfare i requisiti riguardo alle misure di resilienza di cui alla presente direttiva. Al fine di evitare duplicazioni, un'autorità competente dovrebbe poter dichiarare conformi ai requisiti della presente direttiva, in tutto o in parte, misure di resilienza esistenti adottate da un soggetto critico che rispondono ai suoi obblighi di adottare misure tecniche, di sicurezza e organizzative ai sensi della presente direttiva.

(31) I regolamenti (CE) n. 725/2004 ([14]) e (CE) n. 300/2008 ([15]) del Parlamento europeo e del Consiglio e la direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([16]) stabiliscono requisiti applicabili ai soggetti dei settori del trasporto aereo e marittimo per prevenire incidenti causati da atti illeciti, resistere alle conseguenze di tali incidenti e mitigarle. Se le misure imposte ai sensi della presente direttiva sono più ampie in termini di rischi affrontati e di tipi di misure da prendere, i soggetti critici di tali settori dovrebbero rispecchiare, nel loro piano di resilienza o nei documenti equivalenti, le misure adottate ai sensi di tali altri atti giuridici dell'Unione. I soggetti critici dovrebbero prendere in considerazione anche la direttiva 2008/96/CE del Parlamento europeo e del Consiglio ([17]) che introduce una valutazione delle strade a livello di rete per la mappatura del rischio di incidenti e un'ispezione di sicurezza stradale mirata per individuare condizioni pericolose, difetti e problemi che aumentano il rischio di incidenti e lesioni, sulla base di sopralluoghi in strade o in tratti di strada esistenti. Assicurare la protezione e la resilienza dei soggetti critici riveste la massima importanza per il settore ferroviario e, nell'attuare le misure di resilienza ai sensi della presente direttiva, i soggetti critici sono incoraggiati a richiamarsi a linee guida non vincolanti e a documenti su buone prassi sviluppati in aree di lavoro settoriali, come la piattaforma per la sicurezza dei passeggeri ferroviari nell'UE istituita dalla decisione della Commissione 2018/C 232/03 ([18]).

(32) Il rischio che i dipendenti di soggetti critici o i loro contraenti facciano un uso improprio, ad esempio, dei loro diritti di accesso all'interno dell'organizzazione del soggetto critico per nuocere e provocare danni desta sempre maggiori preoccupazioni. Gli Stati membri dovrebbero pertanto precisare le condizioni in base alle quali i soggetti critici sono autorizzati, in casi debitamente motivati e tenendo conto delle valutazioni del rischio dello Stato membro, a presentare richieste di controlli dei precedenti personali per le persone che rientrano in specifiche categorie del loro personale. È opportuno garantire che le pertinenti autorità valutino le richieste entro un lasso di tempo ragionevole e che le trattino conformemente al diritto e alle procedure nazionali, e al diritto dell'Unione pertinente e applicabile, anche in materia di protezione dei dati personali. Al fine di confermare l'identità di una persona oggetto di un controllo dei precedenti personali, è opportuno che gli Stati membri richiedano un documento di identità come un passaporto, una carta d'identità nazionale o una forma di identificazione digitale, conformemente al diritto applicabile.

([14]) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).

([15]) Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

([16]) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).

([17]) Direttiva 2008/96/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, sulla gestione della sicurezza delle infrastrutture stradali (GU L 319 del 29.11.2008, pag. 59).

([18]) Decisione della Commissione, del 29 giugno 2018, che istituisce la piattaforma per la sicurezza dei passeggeri ferroviari nell'UE, 2018/C 232/03 (GU C 232 del 3.7.2018, pag. 10).

I controlli dei precedenti personali dovrebbero includere i registri dei precedenti penali della persona interessata. Gli Stati membri dovrebbero utilizzare il sistema europeo di informazione sui casellari giudiziali conformemente alle procedure stabilite nella decisione quadro 2009/315/GAI del Consiglio ([19]) e, ove pertinente e applicabile, nel regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio ([20]) al fine di ottenere informazioni dai registri dei precedenti penali tenuti da altri Stati membri. Se pertinente e applicabile, gli Stati membri potrebbero inoltre basarsi sul sistema d'informazione Schengen di seconda generazione (SIS II) istituito dal regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio ([21]), su informazioni di intelligence e su qualsiasi altra informazione oggettiva disponibile che possa essere necessaria per determinare l'idoneità della persona interessata a occupare la funzione in relazione alla quale il soggetto critico ha richiesto un controllo dei precedenti personali.

(33) È opportuno stabilire un meccanismo per la notifica di determinati incidenti che consenta alle autorità competenti di reagire rapidamente e adeguatamente agli incidenti e di avere un quadro globale dell'impatto, della natura, delle cause e delle possibili conseguenze di un incidente affrontato dai soggetti critici. I soggetti critici dovrebbero notificare senza indebito ritardo alle autorità competenti gli incidenti che perturbano in modo significativo o possono perturbare in modo significativo la fornitura di servizi essenziali. A meno che siano operativamente impossibilitati a farlo, i soggetti critici dovrebbero effettuare una notifica iniziale entro 24 ore dal momento in cui sono venuti a conoscenza di un incidente. La notifica iniziale dovrebbe contenere solo le informazioni strettamente necessarie per informare l'autorità competente dell'incidente e consentire al soggetto critico di chiedere assistenza, se necessario. Tale notifica dovrebbe indicare, ove possibile, la causa presunta dell'incidente. Gli Stati membri dovrebbero garantire che l'obbligo di effettuare tale notifica iniziale non sottragga le risorse del soggetto critico alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie. La notifica iniziale dovrebbe essere seguita, se del caso, da una relazione dettagliata entro un mese dall'incidente. La relazione dettagliata dovrebbe integrare la notifica iniziale e fornire un quadro più completo dell'incidente.

(34) È opportuno che la normazione resti un processo essenzialmente guidato dal mercato. Potrebbero tuttavia sussistere situazioni in cui è opportuno richiedere l'osservanza di determinate norme. È opportuno che gli Stati membri incoraggino, se utile, l'utilizzo di norme e specifiche tecniche europee e internazionali riguardanti le misure sulla sicurezza e le misure sulla resilienza applicabili ai soggetti critici.

(35) Mentre i soggetti critici, in generale, operano in una rete sempre più interconnessa di fornitura di servizi e di infrastrutture e spesso erogano servizi essenziali in più di uno Stato membro, alcuni di tali soggetti critici sono di particolare rilevanza per l'Unione e per il mercato interno poiché forniscono servizi essenziali a o in sei o più Stati membri, e potrebbero perciò beneficiare di un sostegno specifico a livello dell'Unione. Dovrebbero pertanto essere definite le norme riguardanti le missioni di consulenza a favore di tali soggetti critici di particolare rilevanza europea. Tali norme non pregiudicano le disposizioni sulla vigilanza e sull'esecuzione di cui alla presente direttiva.

(36) Su richiesta motivata della Commissione o di uno o più Stati membri a cui o in cui è fornito il servizio essenziale, qualora sia necessario disporre di ulteriori informazioni per poter consigliare un soggetto critico quanto all'adempimento degli obblighi stabiliti dalla presente direttiva o per poter valutare il rispetto di tali obblighi da parte di un soggetto critico di particolare rilevanza europea, lo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico dovrebbe fornire alla Commissione determinate informazioni di cui alla presente direttiva. In accordo con lo Stato membro che ha individuato il soggetto critico di particolare rilevanza europea come soggetto critico, la Commissione dovrebbe poter organizzare una missione di consulenza per valutare le misure predisposte da tale soggetto. Per garantire che tali missioni di consulenza siano effettuate correttamente dovrebbero essere stabilite disposizioni complementari, in particolare sull'organizzazione e sullo svolgimento delle missioni di consulenza, sul seguito da dare e sugli obblighi dei soggetti critici di particolare

([19]) Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (GU L 93 del 7.4.2009, pag. 23).

([20]) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).

([21]) Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

rilevanza europea interessati. Fermo restando il dovere, per lo Stato membro in cui si svolge la missione di consulenza e per il soggetto critico interessato, di rispettare le disposizioni stabilite dalla presente direttiva, la missione di consulenza dovrebbe essere condotta in ottemperanza delle specifiche norme della legislazione di tale Stato membro, ad esempio sulle precise condizioni da soddisfare per ottenere l'accesso ai locali o ai documenti rilevanti e sul ricorso giurisdizionale. Le specifiche competenze necessarie per tali missioni di consulenza potrebbero, se del caso, essere chieste tramite il centro di coordinamento della risposta alle emergenze istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([22]).

(37) Per sostenere la Commissione e agevolare la cooperazione tra gli Stati membri e lo scambio di informazioni, comprese le migliori prassi, su questioni relative alla presente direttiva, dovrebbe essere istituito un gruppo per la resilienza dei soggetti critici come gruppo di esperti della Commissione. Gli Stati membri dovrebbero adoperarsi per garantire che i rappresentanti designati delle loro autorità competenti nel gruppo per la resilienza dei soggetti critici cooperino in modo efficace ed efficiente, anche designando rappresentanti in possesso, se del caso, di un nulla osta di sicurezza. Il gruppo per la resilienza dei soggetti critici dovrebbe cominciare a espletare le sue funzioni il più rapidamente possibile, in modo da fornire strumenti supplementari per una cooperazione adeguata durante il periodo di recepimento della direttiva, e dovrebbe interagire con altri pertinenti gruppi di lavoro di esperti settoriali.

(38) Il gruppo per la resilienza dei soggetti critici dovrebbe cooperare con il gruppo di cooperazione istituito ai sensi della direttiva (UE) 2022/2555 al fine di sostenere un quadro globale per la resilienza informatica e non informatica dei soggetti critici. Il gruppo per la resilienza dei soggetti critici e il gruppo di cooperazione istituito ai sensi della direttiva (UE) 2022/2555 dovrebbero avviare un dialogo regolare volto a promuovere la cooperazione tra le autorità competenti ai sensi della presente direttiva e le autorità competenti ai sensi della direttiva (UE) 2022/2555 e ad agevolare lo scambio di informazioni, in particolare su temi rilevanti per entrambi i gruppi.

(39) Per conseguire gli obiettivi della presente direttiva, e ferma restando la responsabilità giuridica degli Stati membri e dei soggetti critici quanto al garantire l'ottemperanza ai rispettivi obblighi ivi stabiliti, la Commissione dovrebbe, ove lo ritenga opportuno, sostenere le autorità competenti e i soggetti critici allo scopo di agevolare l'adempimento dei loro rispettivi obblighi. Nel fornire sostegno agli Stati membri e ai soggetti critici nell'attuazione degli obblighi stabiliti dalla presente direttiva la Commissione dovrebbe basarsi sulle strutture e sugli strumenti esistenti, come quelli previsti dal meccanismo di protezione civile dell'Unione, istituito dalla decisione n. 1313/2013/UE, e dalla rete europea di riferimento per la protezione delle infrastrutture critiche. Dovrebbe inoltre informare gli Stati membri in merito alle risorse disponibili a livello dell'Unione, ad esempio nell'ambito del Fondo Sicurezza interna, istituito dal regolamento (UE) 2021/1149 del Parlamento europeo e del Consiglio ([23]), di Orizzonte Europa, istituito dal regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio ([24]), o di altri strumenti pertinenti per la resilienza dei soggetti critici.

(40) Gli Stati membri dovrebbero provvedere affinché le loro autorità competenti dispongano di certi poteri specifici per la corretta applicazione ed esecuzione della presente direttiva nei confronti dei soggetti critici, qualora tali soggetti rientrino nella loro giurisdizione come specificato nella direttiva. Tali poteri dovrebbero includere, in particolare, il potere di effettuare ispezioni e controlli, il potere di vigilanza, il potere di richiedere ai soggetti critici di fornire informazioni e prove riguardanti le misure adottate per adempiere ai loro obblighi e, ove necessario, il potere di emettere provvedimenti per porre rimedio alle violazioni riscontrate. Nell'emettere tali provvedimenti, gli Stati membri non dovrebbero imporre misure che vadano oltre quanto necessario e proporzionato per garantire l'adempimento degli obblighi da parte dei soggetti critici interessati, tenendo conto in particolare della gravità della violazione e della capacità economica del soggetto critico interessato. Più in generale, tali poteri dovrebbero essere accompagnati da garanzie adeguate ed efficaci da specificarsi nella normativa nazionale conformemente alla Carta

([22]) Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).

([23]) Regolamento (UE) 2021/1149 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che istituisce il Fondo Sicurezza interna (GU L 251 del 15.7.2021, pag. 94).

([24]) Regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa e ne stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013 (GU L 170 del 12.5.2021, pag. 1).

dei diritti fondamentali dell'Unione europea. Nel valutare l'ottemperanza di un soggetto critico agli obblighi stabiliti dalla presente direttiva, le autorità competenti ai sensi della presente direttiva dovrebbero poter chiedere alle autorità competenti a norma della direttiva (UE) 2022/2555 di esercitare i propri poteri di vigilanza e di esecuzione nei confronti di un soggetto di cui a tale direttiva individuato come soggetto critico a norma della presente direttiva. Le autorità competenti ai sensi della presente direttiva e le autorità competenti ai sensi della direttiva (UE) 2022/2555 dovrebbero cooperare e scambiarsi informazioni a tal fine.

(41) Al fine di applicare la presente direttiva in modo efficace e coerente, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per integrare la presente direttiva mediante l'elaborazione di un elenco di servizi essenziali. Tale elenco dovrebbe essere utilizzato dalle autorità competenti per effettuare le valutazioni del rischio dello Stato membro e individuare i soggetti critici ai sensi della presente direttiva. Alla luce dell'approccio di armonizzazione minima della presente direttiva, tale elenco non è esaustivo e gli Stati membri potrebbero integrarlo con ulteriori servizi essenziali a livello nazionale al fine di tenere conto delle specificità nazionali nella fornitura di servizi essenziali. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([25]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(42) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione della presente direttiva. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([26]).

(43) Poiché gli obiettivi della presente direttiva, vale a dire garantire che i servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche siano forniti senza impedimenti nel mercato interno ed aumentare la resilienza dei soggetti critici che forniscono tali servizi, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(44) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, ([27]) il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere l'11 agosto 2021.

(45) La direttiva 2008/114/CE dovrebbe pertanto essere abrogata,

([25]) GU L 123 del 12.5.2016, pag. 1.

([26]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([27]) 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).

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. La presente direttiva:

a) stabilisce obblighi in capo agli Stati membri in merito all'adozione di misure specifiche volte a garantire che i servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nell'ambito di applicazione dell'articolo 114 TFUE siano forniti senza impedimenti nel mercato interno, e in particolare obblighi di individuare i soggetti critici e di sostenerli nell'adempimento degli obblighi loro imposti;

b) stabilisce per i soggetti critici obblighi volti a rafforzare la loro resilienza e la loro capacità di fornire servizi di cui alla lettera a) nel mercato interno;

c) stabilisce norme:

   i) riguardanti la vigilanza sui soggetti critici;

   ii) riguardanti l'esecuzione;

   iii) per l'individuazione dei soggetti critici di particolare rilevanza a livello europeo e sulle missioni di consulenza per valutare le misure predisposte da tali soggetti per adempiere ai propri obblighi ai sensi del capo III;

d) stabilisce procedure comuni di cooperazione e comunicazione sull'applicazione della presente direttiva;

e) stabilisce misure intese a raggiungere un livello di resilienza elevato dei soggetti critici al fine di garantire la fornitura di servizi essenziali nell'Unione e migliorare il funzionamento del mercato interno.

2. Fatto salvo l'articolo 8 della presente direttiva, la presente direttiva non si applica alle materie disciplinate dalla direttiva (UE) 2022/2555 In considerazione della relazione tra la sicurezza fisica e la cibersicurezza dei soggetti critici, gli Stati membri assicurano che la presente direttiva e la direttiva (UE) 2022/2555 siano attuate in modo coordinato.

3. Qualora le disposizioni di atti giuridici settoriali dell'Unione richiedano ai soggetti critici di adottare misure per rafforzare la propria resilienza e tali requisiti siano riconosciuti dagli Stati membri come almeno equivalenti ai corrispondenti obblighi stabiliti dalla presente direttiva, non si applicano le pertinenti disposizioni della presente direttiva, comprese le disposizioni in materia di vigilanza ed esecuzione di cui al capo VI.

4. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione o nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti in conformità della presente direttiva solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e la sicurezza e gli interessi commerciali dei soggetti critici, nel rispetto della sicurezza degli Stati membri.

5. La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e la difesa e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

6. La presente direttiva non si applica agli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati.

7. Gli Stati membri possono decidere che l'articolo 11 e i capi III, IV e VI, in tutto o in parte, non si applichino a specifici soggetti critici operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui al paragrafo 6 del presente articolo.

8. Gli obblighi definiti nella presente direttiva non comportano la comunicazione di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

9. La presente direttiva si applica fermo restando il diritto dell'Unione in materia di protezione dei dati personali, in particolare le disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([28]) e della direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([29]).

Articolo 2

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) «soggetto critico»: un soggetto pubblico o privato che è stato individuato da uno Stato membro a ai sensi dell'articolo 6 come appartenente a una delle categorie di cui alla terza colonna della tabella di cui all'allegato;

2) «resilienza»: la capacità di un soggetto critico di prevenire, attenuare, assorbire un incidente, di proteggersi da esso, di rispondervi, di resistervi, di adattarvisi e di ripristinare le proprie capacità operative;

3) «incidente»: un evento che può perturbare in modo significativo, o che perturba, la fornitura di un servizio essenziale, inclusi i casi in cui si ripercuote negativamente sui sistemi nazionali che salvaguardano lo Stato di diritto;

4) «infrastruttura critica»: un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di un elemento, di un impianto, di un'attrezzatura, di una rete o di un sistema, necessari per la fornitura di un servizio essenziale;

5) «servizio essenziale»: un servizio fondamentale per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente;

6) «rischio»: la potenziale perdita o perturbazione causata da un incidente e deve essere espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi l'incidente;

7) «valutazione del rischio »: l'intero processo volto a determinare la natura e la portata di un rischio individuando e analizzando potenziali minacce, vulnerabilità e pericoli pertinenti che potrebbero causare un incidente e valutando la potenziale perdita o perturbazione della fornitura di un servizio essenziale causata da tale incidente;

8) «norma»: una norma ai sensi dell'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([30]);

([28]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([29]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([30]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

9) «specifica tecnica»: una specifica tecnica ai sensi dell'articolo 2, punto 4, del regolamento (UE) n. 1025/2012;

10) «ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, esclusi il settore della giustizia, i parlamenti e le banche centrali, che soddisfa i criteri seguenti:

a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

b) è dotato di personalità giuridica o è autorizzato per legge ad agire per conto di un altro soggetto dotato di personalità giuridica;

c) è finanziato in modo maggioritario da autorità statali o da altri organismi di diritto pubblico a livello centrale; la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata da autorità statali o da altri organismi di diritto pubblico a livello centrale;

d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle persone, delle merci, dei servizi o dei capitali.

Articolo 3

Armonizzazione minima

La presente direttiva non preclude agli Stati membri di adottare o mantenere in vigore disposizioni di diritto nazionale atte a conseguire un livello di resilienza più elevato dei soggetti critici, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.

CAPO II

QUADRI NAZIONALI PER LA RESILIENZA DEI SOGGETTI CRITICI

Articolo 4

Strategia per la resilienza dei soggetti critici

1. A seguito di una consultazione aperta, per quanto praticamente possibile, ai pertinenti portatori di interessi, entro il 17 gennaio 2026 ogni Stato membro adotta una strategia per rafforzare la resilienza dei soggetti critici («strategia»). Sulla base di pertinenti strategie a livello nazionale e settoriale, piani o documenti analoghi esistenti, la strategia definisce gli obiettivi e le misure strategici per conseguire e mantenere un livello elevato di resilienza da parte dei soggetti critici e contempla almeno i settori di cui all'allegato.

2. Ciascuna strategia contiene almeno gli elementi seguenti:

a) obiettivi strategici e priorità per aumentare la resilienza complessiva dei soggetti critici tenendo conto delle dipendenze e interdipendenze transfrontaliere e intersettoriali;

b) un quadro di governance per la realizzazione di tali obiettivi strategici e priorità, che comprenda una descrizione dei ruoli e delle responsabilità delle diverse autorità, dei diversi soggetti critici e delle altre parti coinvolte nell'attuazione della strategia;

c) una descrizione delle misure necessarie per aumentare la resilienza complessiva dei soggetti critici, che comprenda una descrizione della valutazione del rischio di cui all'articolo 5;

d) una descrizione del processo di individuazione dei soggetti critici;

e) una descrizione del processo volto a sostenere i soggetti critici in conformità del presente capo, comprese le misure per rafforzare la cooperazione tra il settore pubblico, da un lato, e il settore privato e i soggetti pubblici e privati, dall'altro;

f) un elenco delle principali autorità e dei pertinenti portatori di interessi, diversi dai soggetti critici, coinvolti nell'attuazione della strategia;

g) un quadro strategico per il coordinamento tra le autorità competenti ai sensi della presente direttiva («autorità competenti») e le autorità competenti ai sensi della direttiva (UE) 2022/2555 ai fini della condivisione delle informazioni sui rischi di cibersicurezza, sulle minacce e sugli incidenti informatici nonché sui rischi, sulle minacce e sugli incidenti non informatici e ai fini dello svolgimento di compiti di vigilanza;

h) una descrizione delle misure già in vigore volte ad agevolare l'attuazione degli obblighi di cui al capo III della presente direttiva da parte delle piccole e medie imprese ai sensi dell'allegato della raccomandazione 2003/361/CE della Commissione ([31]), che gli Stati membri in questione hanno individuato come soggetti critici.

A seguito di una consultazione aperta, per quanto praticamente possibile, ai pertinenti portatori di interessi, gli Stati membri aggiornano le loro strategie almeno ogni quattro anni.

3. Gli Stati membri comunicano alla Commissione le loro strategie, e i relativi aggiornamenti sostanziali, entro tre mesi dalla loro adozione.

Articolo 5

Valutazione del rischio da parte degli Stati membri

1. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 23, entro il 17 novembre 2023, al fine di integrare la presente direttiva stabilendo un elenco non esaustivo dei servizi essenziali nei settori e nei sottosettori di cui all'allegato. Le autorità competenti utilizzano tale elenco dei servizi essenziali per effettuare una valutazione del rischio («valutazione del rischio dello Stato membro») entro il 17 gennaio 2026 e successivamente ogniqualvolta necessario e almeno ogni quattro anni. Le autorità competenti utilizzano le valutazioni del rischio dello Stato membro per individuare i soggetti critici ai sensi dell'articolo 6 e per aiutare tali soggetti critici ad adottare misure ai sensi dell'articolo 13.

La valutazione del rischio dello Stato membro tiene conto dei rischi rilevanti, naturali e di origine umana, compresi quelli di natura intersettoriale o transfrontaliera, gli incidenti, le catastrofi naturali, le emergenze di sanità pubblica, le minacce ibride o altre minacce antagoniste, inclusi i reati di terrorismo di cui alla direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio ([32]).

2. Nel procedere alla valutazione del rischio dello Stato membro, gli Stati membri prendono in considerazione almeno gli elementi seguenti:

a) la valutazione generale del rischio effettuata ai sensi dell'articolo 6, paragrafo 1, della decisione n. 1313/2013/UE;

b) altre valutazioni del rischio rilevanti, svolte in conformità dei requisiti dei pertinenti atti giuridici settoriali dell'Unione, inclusi i regolamenti (UE) 2017/1938 ([33]) e (UE) 2019/941 ([34]) del Parlamento europeo e del Consiglio e le direttive 2007/60/CE ([35]) e 2012/18/UE ([36]) del Parlamento europeo e del Consiglio;

([31]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

([32]) Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU L 88 del 31.3.2017, pag. 6).

([33]) Regolamento (UE) 2017/1938 del Parlamento europeo e del Consiglio, del 25 ottobre 2017, concernente misure volte a garantire la sicurezza dell'approvvigionamento di gas e che abroga il regolamento (UE) n. 994/2010 (GU L 280 del 28.10.2017, pag. 1).

([34]) Regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sulla preparazione ai rischi nel settore dell'energia elettrica e che abroga la direttiva 2005/89/CE (GU L 158 del 14.6.2019, pag. 1).

([35]) Direttiva 2007/60/CE del Parlamento europeo e del Consiglio, del 23 ottobre 2007, relativa alla valutazione e alla gestione dei rischi di alluvioni (GU L 288 del 6.11.2007, pag. 27).

([36]) Direttiva 2012/18/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sul controllo del pericolo di incidenti rilevanti connessi con sostanze pericolose, recante modifica e successiva abrogazione della direttiva 96/82/CE del Consiglio (GU L 197 del 24.7.2012, pag. 1).

c) i rischi pertinenti derivanti dalla misura in cui i settori di cui all'allegato dipendono l'uno dall'altro, e anche dalla misura in cui essi dipendono da soggetti situati in altri Stati membri e paesi terzi, e l'impatto che una perturbazione significativa in un settore può avere su altri settori, compresi gli eventuali rischi significativi per i cittadini e il mercato interno;

d) ogni informazione su incidenti notificati a norma dell'articolo 15.

Ai fini del primo comma, lettera c), gli Stati membri cooperano con le autorità competenti degli altri Stati membri e le autorità competenti dei paesi terzi, a seconda dei casi.

3. Gli Stati membri mettono a disposizione dei soggetti critici individuati ai sensi dell'articolo 6 gli elementi rilevanti della valutazione del rischio dello Stato membro, se del caso mediante i propri punti di contatto unici. Gli Stati membri garantiscono che le informazioni fornite ai soggetti critici li assistano nell'effettuare la propria valutazione del rischio ai sensi dell'articolo 12 e ad adottare le misure per garantire la propria resilienza ai sensi dell'articolo 13.

4. Entro tre mesi dall'effettuazione della valutazione del rischio dello Stato membro, lo Stato membro trasmette alla Commissione le informazioni pertinenti sui tipi di rischi individuati e sui risultati delle valutazioni del rischio di tale Stato membro, per settore e sottosettore di cui all'allegato.

5. La Commissione, in cooperazione con gli Stati membri, sviluppa un modello comune volontario per la presentazione delle relazioni in ottemperanza con il paragrafo 4.

Articolo 6

Individuazione dei soggetti critici

1. Entro il 17 luglio 2026 ogni Stato membro individua i soggetti critici per i settori e i sottosettori di cui all'allegato.

2. Quando uno Stato membro individua i soggetti critici ai sensi del paragrafo 1, tiene conto dei risultati della propria valutazione del rischio dello Stato membro e della propria strategia e applica tutti i criteri seguenti:

a) il soggetto fornisce uno o più servizi essenziali;

b) il soggetto opera, e la sua infrastruttura critica è situata, sul territorio di tale Stato membro; e

c) un incidente avrebbe effetti negativi rilevanti, determinati in conformità dell'articolo 7, paragrafo 1, sulla fornitura da parte del soggetto di uno o più servizi essenziali, o sulla fornitura di altri servizi essenziali nei settori di cui all'allegato che dipendono da tale o tali servizi essenziali.

3. Ogni Stato membro redige un elenco dei soggetti critici individuati a norma del paragrafo 2 e provvede affinché a tali soggetti critici sia notificato che sono stati individuati come tali entro un mese dall'individuazione stessa. Gli Stati membri informano tali soggetti critici degli obblighi di cui ai capi III e IV e della data a decorrere dalla quale si applicano loro tali obblighi, fatto salvo l'articolo 8. Gli Stati membri informano i soggetti critici dei settori di cui ai punti 3, 4 e 8 della tabella di cui all'allegato che non hanno obblighi di cui ai capi III e IV, salvo misure nazionali diverse.

Il capo III si applica ai soggetti critici interessati 10 mesi dopo la data della notifica di cui al primo comma del presente paragrafo.

4. Gli Stati membri provvedono affinché le rispettive autorità competenti ai sensi della presente direttiva notifichino alle autorità competenti di cui alla direttiva (UE) 2022/2555 l'identità dei soggetti critici individuati ai sensi del presente articolo entro un mese dall'individuazione. Tale notifica specifica, ove applicabile, che i soggetti critici interessati sono soggetti dei settori di cui ai punti 3, 4 e 8 della tabella di cui all'allegato della presente direttiva e non hanno obblighi di cui ai capi III e IV della stessa.

5. Quando necessario e, in ogni caso, almeno ogni quattro anni, gli Stati membri riesaminano e, se del caso, aggiornano l'elenco dei soggetti critici individuati di cui al paragrafo 3. Qualora tali aggiornamenti portino all'individuazione di soggetti critici ulteriori, a questi ultimi si applicano i paragrafi 3 e 4. Gli Stati membri provvedono inoltre affinché i soggetti non più individuati come critici a seguito di un aggiornamento ricevano notifica di tale fatto in tempo utile e del fatto che non debbano più adempiere agli obblighi di cui al capo III a decorrere dalla data di ricevimento di tale notifica.

6. La Commissione, in cooperazione con gli Stati membri, elabora raccomandazioni e linee guida non vincolanti volti ad aiutare gli Stati membri a individuare i soggetti critici.

Articolo 7

Effetti negativi rilevanti

1. Nella determinazione della rilevanza degli effetti negativi di cui all'articolo 6, paragrafo 2, lettera c), gli Stati membri tengono conto dei criteri seguenti:

a) il numero di utenti che dipendono dal servizio essenziale fornito dal soggetto interessato;

b) la misura in cui altri settori e sottosettori di cui all'allegato dipendono dal servizio essenziale in questione;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali, sull'ambiente, sulla pubblica sicurezza, sull'incolumità pubblica o sulla salute della popolazione;

d) la quota di mercato del soggetto nel mercato del servizio essenziale o dei servizi essenziali interessati;

e) l'area geografica che potrebbe essere interessata da un incidente, compresi eventuali impatti transfrontalieri, tenendo conto della vulnerabilità associata al grado di isolamento di alcuni tipi di aree geografiche, come quelle insulari, remote o montane;

f) l'importanza del soggetto nel mantenimento di un livello sufficiente del servizio essenziale, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio essenziale.

2. A seguito dell'individuazione dei soggetti critici di cui all'articolo 6, paragrafo 1, ciascuno Stato membro comunica senza indebito ritardo alla Commissione le informazioni seguenti:

a) un elenco dei servizi essenziali in tale Stato membro qualora vi siano servizi essenziali aggiuntivi rispetto all'elenco dei servizi essenziali di cui all'articolo 5, paragrafo 1;

b) il numero di soggetti critici individuati per ciascun settore e sottosettore di cui all'allegato e per ciascun servizio essenziale;

c) le soglie applicate per specificare uno o più criteri di cui al paragrafo 1.

Le soglie di cui al primo comma, lettera c), possono essere presentate come tali o in forma aggregata.

Gli Stati membri comunicano successivamente le informazioni di cui al primo comma quando necessario, e almeno ogni quattro anni.

3. La Commissione, previa consultazione del gruppo per la resilienza dei soggetti critici di cui all'articolo 19, adotta linee guida non vincolanti per agevolare l'applicazione dei criteri di cui al paragrafo 1 del presente articolo, tenendo conto delle informazioni di cui al paragrafo 2 del presente articolo.

Articolo 8

Soggetti critici del settore bancario, delle infrastrutture dei mercati finanziari e delle infrastrutture digitali

Gli Stati membri provvedono affinché l'articolo 11 e i capi III, IV e VI non si applichino ai soggetti critici che hanno individuato nei settori di cui ai punti 3, 4 e 8 della tabella di cui all'allegato. Gli Stati membri possono adottare o mantenere in vigore disposizioni di diritto interno atte a conseguire un livello di resilienza più elevato per tali soggetti critici, a condizione che dette disposizioni siano coerenti con il diritto dell'Unione applicabile.

Articolo 9

Autorità competenti e punto di contatto unico

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della corretta applicazione e, se necessario, dell'esecuzione delle norme della presente direttiva a livello nazionale.

Per quanto riguarda i soggetti critici nei settori di cui ai punti 3 e 4 della tabella di cui all'allegato della presente direttiva, le autorità competenti sono, in linea di principio, le autorità competenti di cui all'articolo 46 del regolamento (UE) 2022/2554 Per quanto riguarda i soggetti critici nel settore di cui al punto 8 della tabella di cui all'allegato della presente direttiva, le autorità competenti sono, in linea di principio, le autorità competenti di cui alla direttiva (UE) 2022/2555 Gli Stati membri possono designare una diversa autorità competente per i settori di cui ai punti 3, 4 e 8 della tabella figurante nell'allegato della presente direttiva in conformità dei quadri nazionali esistenti.

Qualora designino o istituiscano più di un'autorità competente, gli Stati membri definiscono chiaramente i compiti di ciascuna delle autorità interessate e provvedono affinché esse cooperino efficacemente per svolgerli a norma della presente direttiva, anche per quanto riguarda la designazione e le attività del punto di contatto unico di cui al paragrafo 2.

2. Ciascuno Stato membro designa o istituisce un punto di contatto unico, che svolga una funzione di collegamento allo scopo di garantire la cooperazione transfrontaliera con i punti di contatto unici di altri Stati membri e con il gruppo per la resilienza dei soggetti critici di cui all'articolo 19 («punto di contatto unico»). Se del caso, uno Stato membro designa il suo punto di contatto unico all'interno di una autorità competente. Se del caso, uno Stato membro può provvedere affinché il suo punto di contatto unico svolga anche una funzione di collegamento con la Commissione e garantisca la cooperazione con i paesi terzi.

3. Entro il 17 luglio 2028, e successivamente ogni due anni, i punti di contatto unici trasmettono alla Commissione e al gruppo per la resilienza dei soggetti critici di cui all'articolo 19 una relazione di sintesi in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati, e alle azioni intraprese a norma dell'articolo 15, paragrafo 3.

La Commissione, in cooperazione con il gruppo per la resilienza dei soggetti critici, sviluppa un modello comune per la presentazione delle relazioni. Le autorità competenti possono utilizzare, su base volontaria, tale modello comune per la presentazione delle relazioni ai fini della presentazione delle relazioni di sintesi di cui al primo comma.

4. Ciascuno Stato membro provvede affinché la propria autorità competente e il punto di contatto unico dispongano dei poteri e delle risorse finanziarie, umane e tecniche adeguate a svolgere in modo efficace ed efficiente i compiti che sono loro assegnati.

5. Ciascuno Stato membro provvede affinché la propria autorità competente, ove opportuno e conformemente al diritto dell'Unione e al diritto nazionale, si consulti e cooperi con le altre autorità nazionali competenti, comprese quelle responsabili della protezione civile, delle attività di contrasto e della protezione dei dati personali, e con i soggetti critici e le parti interessate pertinenti.

6. Ciascuno Stato membro provvede affinché la propria autorità competente ai sensi della presente direttiva cooperi e scambi informazioni con le autorità competenti di cui alla direttiva (UE) 2022/2555 sui rischi di cibersicurezza, sulle minacce e sugli incidenti informatici e sui rischi, sulle minacce e sugli incidenti non informatici che hanno ripercussioni sui soggetti critici, anche per quanto riguarda le pertinenti misure adottate dalla rispettiva autorità competente e dalle autorità competenti di cui alla direttiva (UE) 2022/2555

7. Entro tre mesi dalla designazione o istituzione dell'autorità competente e del punto di contatto unico, ogni Stato membro notifica alla Commissione la loro identità e i loro compiti e responsabilità ai sensi della presente direttiva e i loro dati di contatto, e qualsiasi ulteriore modifica dei medesimi. Gli Stati membri informano la Commissione qualora decidano di nominare autorità diverse dalle autorità competenti di cui al paragrafo 1, secondo comma, quali autorità competenti in relazione ai soggetti critici nei settori di cui ai punti 3, 4 e 8 della tabella di cui all'allegato. Ogni Stato membro rende pubblica l'identità della rispettiva autorità competente e del punto di contatto unico.

8. La Commissione rende disponibile al pubblico un elenco dei punti di contatto unici.

Articolo 10

Sostegno degli Stati membri ai soggetti critici

1. Gli Stati membri sostengono i soggetti critici nel rafforzamento della loro resilienza. Tale sostegno può comportare l'elaborazione di materiali e metodologie di orientamento, aiuto nell'organizzazione di esercitazioni per testare la propria resilienza nonché la prestazione di consulenza e di corsi di formazione per il personale dei soggetti critici. Fatte salve le norme applicabili in materia di aiuti di Stato, gli Stati membri possono fornire risorse finanziarie ai soggetti critici, ove ciò sia necessario e giustificato da obiettivi di interesse pubblico.

2. Ogni Stato membro provvede affinché la rispettiva autorità competente cooperi e scambi informazioni e buone prassi con i soggetti critici dei settori di cui all'allegato.

3. Gli Stati membri agevolano la condivisione volontaria di informazioni fra i soggetti critici in relazione alle materie disciplinate dalla presente direttiva, conformemente al diritto dell'Unione e al diritto nazionale, riguardo, in particolare, alle informazioni classificate e sensibili, alla concorrenza e alla protezione dei dati personali.

Articolo 11

Cooperazione tra Stati membri

1. Ogniqualvolta ciò sia opportuno, gli Stati membri si consultano reciprocamente in merito ai soggetti critici al fine di un'applicazione coerente della presente direttiva. Tali consultazioni si svolgono, in particolare, per i soggetti critici che:

a) utilizzano infrastrutture critiche fisicamente collegate tra due o più Stati membri;

b) fanno parte di strutture societarie collegate o associate a soggetti critici in altri Stati membri;

c) sono stati individuati come soggetti critici in uno Stato membro e forniscono servizi essenziali ad altri Stati membri o in altri Stati membri.

2. Le consultazioni di cui al paragrafo 1 sono intese a rafforzare la resilienza dei soggetti critici e, ove possibile, a ridurre gli oneri amministrativi a loro carico.

CAPO III

RESILIENZA DEI SOGGETTI CRITICI

Articolo 12

Valutazione del rischio da parte dei soggetti critici

1. Fatto salvo il termine di cui all'articolo 6, paragrafo 3, secondo comma, gli Stati membri provvedono affinché i soggetti critici effettuino una valutazione del rischio, entro nove mesi dal ricevimento della notifica di cui all'articolo 6, paragrafo 3, e successivamente quando necessario e almeno ogni quattro anni, valutino, basandosi sulle valutazioni del rischio degli Stati membri e su altre fonti di informazioni pertinenti, al fine di valutare tutti i rischi rilevanti che potrebbero perturbare la fornitura dei loro servizi essenziali («valutazione del rischio dei soggetti critici»).

2. Le valutazioni del rischio dei soggetti critici tengono conto di tutti i rischi rilevanti naturali e di origine umana che potrebbero causare un incidente, compresi quelli di natura intersettoriale o transfrontaliera, gli incidenti, le catastrofi naturali, le emergenze di sanità pubblica, le minacce ibride e altre minacce antagoniste, inclusi i reati di terrorismo di cui alla direttiva (UE) 2017/541. La valutazione del rischio dei soggetti critici tiene conto della misura in cui altri settori di cui all'allegato dipendono dal servizio essenziale fornito dal soggetto critico e della misura in cui tale soggetto critico dipende dai servizi essenziali forniti da altri soggetti in taluni altri settori, se del caso, anche negli Stati membri e nei paesi terzi vicini.

Qualora un soggetto critico abbia effettuato altre valutazioni del rischio o redatto documenti conformemente agli obblighi previsti da altri atti giuridici pertinenti per la propria valutazione del rischio dei soggetti critici, può utilizzare tali valutazioni e documenti per soddisfare i requisiti stabiliti al presente articolo. Nell'esercizio delle sue funzioni di vigilanza, l'autorità competente può decidere di dichiarare conforme, in tutto o in parte, ai requisiti del presente articolo una valutazione del rischio esistente di un soggetto critico che affronta i rischi e il grado di dipendenza di cui al primo comma del presente paragrafo.

Articolo 13

Misure di resilienza dei soggetti critici

1. Gli Stati membri provvedono affinché i soggetti critici adottino misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la propria resilienza, in base alle informazioni pertinenti fornite dagli Stati membri in merito alla valutazione del rischio dello Stato membro e in base ai risultati della valutazione del rischio del soggetto critico, incluse misure necessarie per:

a) evitare il verificarsi di incidenti, prendendo debitamente in considerazione le misure di riduzione del rischio di catastrofi e di adattamento ai cambiamenti climatici;

b) assicurare un'adeguata protezione fisica dei propri siti e delle infrastrutture critiche prendendo debitamente in considerazione, ad esempio, recinzioni, barriere, strumenti e routine di controllo del perimetro, impianti di rilevamento e controllo degli accessi;

c) contrastare e resistere alle conseguenze degli incidenti e mitigarle, prendendo debitamente in considerazione procedure e protocolli di gestione dei rischi e delle crisi e pratiche di allerta;

d) ripristinare le proprie capacità operative in caso di incidenti, prendendo debitamente in considerazione misure di continuità operativa e l'individuazione di catene di approvvigionamento alternative al fine di ripristinare la fornitura del servizio essenziale;

e) assicurare un'adeguata gestione della sicurezza del personale, prendendo debitamente in considerazione misure quali la definizione di categorie di personale che svolgono funzioni critiche, l'introduzione di autorizzazioni di accesso ai siti e alle infrastrutture critiche così come alle informazioni sensibili, istituendo procedure per i controlli dei precedenti personali in conformità dell'articolo 14 e designando le categorie di persone tenute a sottoporsi a tali controlli dei precedenti personali, e definendo adeguati requisiti di formazione e qualifiche;

f) sensibilizzare il personale interessato in merito alle misure di cui alle lettere da a) ad e), prendendo debitamente in considerazione corsi di formazione, materiale informativo ed esercitazioni.

Ai fini del primo comma, lettera e), gli Stati membri provvedono affinché i soggetti critici tengano conto del personale dei fornitori esterni di servizi nel definire le categorie di personale che svolgono funzioni critiche.

2. Gli Stati membri provvedono affinché i soggetti critici predispongano e applichino un piano di resilienza o un documento o documenti equivalenti, in cui siano descritte le misure di cui al paragrafo 1. Qualora i soggetti critici abbiano redatto documenti o adottato misure conformemente agli obblighi previsti da altri atti giuridici pertinenti per le misure stabilite al paragrafo 1, essi possono utilizzare tali documenti e misure per soddisfare i requisiti stabiliti dal presente articolo. Nell'esercizio delle sue funzioni di vigilanza, l'autorità competente può dichiarare conformi, in tutto o in parte, agli obblighi di cui a presente articolo le misure esistenti di rafforzamento della resilienza di un soggetto critico che affrontano in modo adeguato e proporzionato le misure tecniche, di sicurezza e organizzative di cui al paragrafo 1.

3. Gli Stati membri provvedono affinché ciascun soggetto critico designi un funzionario di collegamento o equivalente come punto di contatto con le autorità competenti.

4. Su richiesta dello Stato membro che ha individuato il soggetto critico, e con l'accordo del soggetto critico interessato, la Commissione organizza missioni di consulenza, conformemente alle disposizioni di cui all'articolo 18, paragrafi 6, 8 e 9, per consigliare il soggetto critico riguardo all'adempimento degli obblighi di cui al capo III. La missione di consulenza riferisce i suoi risultati alla Commissione, a tale Stato membro e al soggetto critico interessato.

5. La Commissione, previa consultazione del gruppo per la resilienza dei soggetti critici di cui all'articolo 19, adotta linee guida non vincolanti per specificare ulteriormente le misure tecniche, di sicurezza e organizzative che possono essere adottate a norma del paragrafo 1 del presente articolo.

6. La Commissione adotta atti di esecuzione per definire le necessarie specifiche tecniche e metodologiche relative all'applicazione delle misure di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 24, paragrafo 2.

Articolo 14

Controlli dei precedenti personali

1. Gli Stati membri precisano le condizioni in base alle quali il soggetto critico è autorizzato, in casi debitamente motivati e tenendo conto della valutazione del rischio dello Stato membro, a presentare richieste di controlli dei precedenti personali per le persone che:

a) rivestono ruoli sensibili all'interno del soggetto critico o a vantaggio di quest'ultimo, segnatamente in relazione alla resilienza del soggetto critico;

b) sono autorizzate ad accedere — direttamente o a distanza — ai suoi siti e ai suoi sistemi informatici o di controllo, anche in relazione alla sicurezza del soggetto critico;

c) sono presi in considerazione per l'assunzione in ruoli che rientrano nei criteri di cui alle lettere a) o b).

2. Le richieste di cui al paragrafo 1 del presente articolo sono valutate entro un lasso di tempo ragionevole e trattate conformemente al diritto e alle procedure nazionali, e al diritto dell'Unione pertinente e applicabile, compresi il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([37]). I controlli dei precedenti personali sono proporzionati e strettamente limitati a quanto necessario e sono effettuati al solo scopo di valutare un potenziale rischio per la sicurezza del soggetto critico interessato.

3. Il controllo dei precedenti personali di cui al paragrafo 1, come minimo:

a) conferma l'identità della persona che è soggetta al controllo dei precedenti personali;

b) verifica i precedenti penali di tale persona per quanto riguarda reati rilevanti ai fini di uno specifico ruolo.

Nell'effettuare i controlli dei precedenti personali, gli Stati membri, si avvalgono del sistema europeo di informazione sui casellari giudiziali conformemente alle procedure stabilite nella decisione quadro 2009/315/GAI e, ove pertinente e applicabile, nel regolamento (UE) 2019/816 per ottenere le informazioni sui precedenti penali in possesso di altri Stati membri. Le autorità centrali di cui all'articolo 3, paragrafo 1, della decisione quadro 2009/315/GAI e all'articolo 3, punto 5), del regolamento (UE) 2019/816 forniscono risposte alle richieste di informazioni in questione entro 10 giorni lavorativi dalla data di ricevimento della richiesta, conformemente all'articolo 8, paragrafo 1, della decisione quadro 2009/315/GAI.

([37]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

Articolo 15

Notifica degli incidenti

1. Gli Stati membri provvedono affinché i soggetti critici notifichino senza indebito ritardo all'autorità competente gli incidenti che perturbano o possono perturbare in modo significativo in modo significativo la fornitura di servizi essenziali. Gli Stati membri provvedono affinché, a meno che non siano operativamente impossibilitati a farlo, i soggetti critici effettuino una notifica iniziale entro 24 ore dal momento in cui vengono a conoscenza di un incidente, seguita, ove opportuno, da una relazione finale dettagliata al più tardi dopo un mese. Per determinare la rilevanza della perturbazione si tiene conto in particolare dei parametri seguenti:

a) numero e percentuale di utenti interessati dalla perturbazione;

b) durata della perturbazione;

c) area geografica interessata dalla perturbazione, tenendo conto dell'eventuale isolamento geografico di tale area.

Qualora un incidente abbia o possa avere un impatto significativo sulla continuità della fornitura dei servizi essenziali a o in sei o più Stati membri, le autorità competenti degli Stati membri interessati dall'incidente notificano tale incidente alla Commissione.

2. Le notifiche di cui al paragrafo 1, primo comma, includono tutte le informazioni disponibili necessarie per consentire all'autorità competente di comprendere la natura, la causa e le possibili conseguenze dell'incidente, comprese tutte le informazioni disponibili necessarie alla determinazione di un suo eventuale impatto transfrontaliero. Tali notifiche non espongono i soggetti critici a una maggiore responsabilità.

3. Sulla base delle informazioni fornite da un soggetto critico in una notifica di cui al paragrafo 1, l'autorità competente, tramite il punto di contatto unico, informa il punto di contatto unico degli altri Stati membri interessati nel caso in cui l'incidente abbia, o possa avere, un impatto significativo sui soggetti critici e sulla continuità dei servizi essenziali a o in uno o più altri Stati membri.

I punti di contatto unici che trasmettono e ricevono informazioni a norma del primo comma, trattano, conformemente al diritto dell'Unione o al diritto nazionale, tali informazioni rispettandone la riservatezza e tutelando la sicurezza e gli interessi commerciali del soggetto critico interessato.

4. Il più rapidamente possibile a seguito di una notifica di cui al paragrafo 1, l'autorità competente interessata fornisce al soggetto critico interessato informazioni rilevanti sul seguito dato, comprese informazioni che possano supportare un'efficace risposta di tale soggetto critico all'incidente in questione. Gli Stati membri informano il pubblico qualora ritengano che sia nell'interesse pubblico farlo.

Articolo 16

Norme

Per promuovere l'attuazione convergente della presente direttiva, gli Stati membri, laddove opportuno e senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali riguardanti le misure sulla sicurezza e le misure sulla resilienza applicabili ai soggetti critici.

CAPO IV

SOGGETTI CRITICI DI PARTICOLARE RILEVANZA EUROPEA

Articolo 17

Individuazione dei soggetti critici di particolare rilevanza europea

1. Un soggetto è considerato soggetto critico di particolare rilevanza europea se:

a) è stato individuato come soggetto critico ai sensi dell'articolo 6, paragrafo 1;

b) fornisce servizi essenziali identici o analoghi a o in sei o più Stati membri; e

c) è stato notificato ai sensi del paragrafo 3.

2. Gli Stati membri provvedono affinché un soggetto critico, a seguito della notifica di cui all'articolo 6, paragrafo 3, comunichi alla rispettiva autorità competente se fornisce servizi essenziali a o in sei o più Stati membri. In tal caso, gli Stati membri provvedono affinché il soggetto critico comunichi alla rispettiva autorità competente quali servizi essenziali fornisce a o in tali Stati membri e a quali o in quali Stati membri fornisce tali servizi essenziali. Lo Stato membro notifica alla Commissione, senza indebito ritardo, l'identità di tali soggetti critici e le informazioni che essi forniscono ai sensi del presente paragrafo.

La Commissione si consulta con l'autorità competente dello Stato membro che ha individuato un soggetto critico di cui al primo comma, l'autorità competente di altri Stati membri interessati e il soggetto critico in questione. Nel corso di tali consultazioni ciascuno Stato membro comunica alla Commissione se ritiene che i servizi forniti a tale Stato membro dal soggetto critico siano servizi essenziali.

3. Se stabilisce, sulla base delle consultazioni di cui al paragrafo 2 del presente articolo, che il soggetto critico interessato fornisce servizi essenziali a o in sei o più Stati membri, la Commissione comunica a tale soggetto critico, tramite la relativa autorità competente, la sua individuazione come soggetto critico di particolare rilevanza europea e informa tale soggetto critico degli obblighi ai quali è assoggettato ai sensi del presente capo e della data a decorrere dalla quale si applicano tali obblighi. Una volta che la Commissione ha informato l'autorità competente della sua decisione di considerare un soggetto critico come un soggetto critico di particolare rilevanza europea, l'autorità competente trasmette tale notifica senza indebito ritardo a tale soggetto critico.

4. Il presente capo si applica al soggetto critico di particolare rilevanza europea interessato a decorrere dalla data di ricevimento della notifica di cui al paragrafo 3 del presente articolo.

Articolo 18

Missioni di consulenza

1. Su richiesta dello Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1, la Commissione organizza una missione di consulenza per valutare le misure predisposte da tale soggetto critico per adempiere ai propri obblighi di cui al capo III.

2. Di propria iniziativa o su richiesta di uno o più Stati membri a cui o in cui è fornito il servizio essenziale, e a condizione che lo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1, sia d'accordo, la Commissione organizza una missione di consulenza di cui al paragrafo 1 del presente articolo.

3. Su richiesta motivata della Commissione o di uno o più Stati membri a cui o in cui è fornito il servizio essenziale, lo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1 fornisce alla Commissione:

a) le parti pertinenti della valutazione del rischio del soggetto critico;

b) un elenco delle pertinenti misure adottate ai sensi dell'articolo 13;

c) le azioni di vigilanza o di esecuzione, comprese le valutazioni di conformità o i provvedimenti emessi, che la relativa autorità competente ha intrapreso nei confronti di tale soggetto critico ai sensi degli articoli 21 e 22.

4. Entro tre mesi dalla sua conclusione, la missione di consulenza riferisce i suoi risultati alla Commissione, allo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1, allo Stato membro a cui o in cui è fornito il servizio essenziale e al soggetto critico interessato.

Gli Stati membri a cui o in cui è fornito il servizio essenziale analizzano la relazione di cui al primo comma e, qualora necessario, danno indicazioni alla Commissione sull'adempimento o meno degli obblighi di cui al capo III da parte del soggetto critico di particolare rilevanza europea interessato e, se del caso, su quali misure potrebbero essere adottate per migliorare la resilienza di tale soggetto critico.

Sulla base dell'indicazione di cui al secondo comma del presente paragrafo, la Commissione comunica allo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1, agli Stati membri a cui o in cui è fornito il servizio essenziale e a tale soggetto critico il suo parere sull'adempimento o meno degli obblighi di cui al capo III da parte di tale soggetto critico e, se del caso, quali misure potrebbero essere adottate per migliorare la sua resilienza.

Lo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1 provvede affinché la sua autorità competente e il soggetto critico interessato tengano conto del parere di cui al terzo comma del presente paragrafo e fornisce alla Commissione e agli Stati membri a cui o in cui è fornito il servizio essenziale informazioni sulle misure adottate a seguito di tale parere.

5. Ogni missione di consulenza è composta da esperti dello Stato membro in cui è situato il soggetto critico di particolare rilevanza europea, da esperti degli Stati membri a cui o in cui è fornito il servizio essenziale, e da rappresentanti della Commissione. Tali Stati membri possono proporre i loro candidati. La Commissione, previa consultazione dello Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1, seleziona e nomina i membri di ciascuna missione di consulenza in base alla loro capacità professionale e garantendo, ove possibile, una rappresentanza equilibrata sotto il profilo geografico di tutti gli Stati membri interessati. Ogniqualvolta necessario, i membri della missione di consulenza devono essere in possesso di un valido e appropriato nulla osta di sicurezza. La Commissione sostiene i costi relativi alla partecipazione alle missioni di consulenza.

La Commissione organizza il programma di ciascuna missione di consulenza consultandosi con i membri della missione di consulenza in questione e d'accordo con lo Stato membro che ha individuato un soggetto critico di particolare rilevanza europea come soggetto critico ai sensi dell'articolo 6, paragrafo 1.

6. La Commissione adotta un atto di esecuzione che stabilisce le norme relative alle modalità procedurali per la presentazione di richieste per l'organizzazione di missioni di consulenza, per il trattamento di tali richieste, per lo svolgimento delle missioni di consulenza e per le attinenti relazioni e per il trattamento della comunicazione del parere della Commissione di cui al paragrafo 4, terzo comma del presente articolo e delle misure adottate, tenendo in debito conto la riservatezza e la sensibilità aziendale delle informazioni interessate. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 24, paragrafo 2.

7. Gli Stati membri provvedono affinché i soggetti critici di particolare rilevanza europea forniscano alle missioni di consulenza accesso alle informazioni e ai sistemi e impianti relativi alla fornitura dei loro servizi essenziali che sono necessari per lo svolgimento della missione di consulenza interessata.

8. Le missioni di consulenza sono svolte conformemente al diritto nazionale applicabile dello Stato membro in cui hanno luogo, nel rispetto della responsabilità di tale Stato membro in materia di sicurezza nazionale e della tutela dei propri interessi di sicurezza.

9. Nell'organizzare le missioni di consulenza la Commissione tiene conto delle relazioni sulle ispezioni da essa effettuate ai sensi dei regolamenti (CE) n. 725/2004 e (CE) n. 300/2008 e delle relazioni sui controlli da essa svolti ai sensi della direttiva 2005/65/CE in merito al soggetto critico interessato.

10. La Commissione informa il gruppo per la resilienza dei soggetti critici di cui all'articolo 19 ogniqualvolta è organizzata una missione di consulenza. Lo Stato membro in cui si è svolta la missione di consulenza e la Commissione informano inoltre il gruppo per la resilienza dei soggetti critici in merito ai principali risultati della missione di consulenza e alle lezioni apprese al fine di promuovere l'apprendimento reciproco.

CAPO V

COOPERAZIONE E COMUNICAZIONE

Articolo 19

Gruppo per la resilienza dei soggetti critici

1. È istituito il gruppo per la resilienza dei soggetti critici. Il gruppo per la resilienza dei soggetti critici sostiene la Commissione e agevola la cooperazione tra gli Stati membri e lo scambio di informazioni su questioni attinenti alla presente direttiva.

2. Il gruppo per la resilienza dei soggetti critici è composto da rappresentanti degli Stati membri e della Commissione in possesso, se del caso, di un nulla osta di sicurezza. Qualora ciò sia rilevante per lo svolgimento dei suoi compiti, esso può invitare i portatori di interessi a partecipare ai suoi lavori. Su richiesta del Parlamento europeo, la Commissione può invitare esperti del Parlamento europeo a partecipare alle riunioni del gruppo per la resilienza dei soggetti critici.

Il rappresentante della Commissione presiede il gruppo per la resilienza dei soggetti critici.

3. Il gruppo per la resilienza dei soggetti critici ha i compiti seguenti:

a) assistere la Commissione nel fornire aiuto agli Stati membri per il rafforzamento della loro capacità di contribuire a garantire la resilienza dei soggetti critici ai sensi della presente direttiva;

b) analizzare le strategie al fine di individuare le migliori prassi in relazione alle stesse;

c) facilitare lo scambio di migliori prassi per quanto riguarda l'individuazione dei soggetti critici da parte degli Stati membri ai sensi dell'articolo 6, paragrafo 1, anche in relazione alle dipendenze transfrontaliere e intersettoriali e per quanto riguarda i rischi e gli incidenti;

d) se del caso, contribuire, per questioni relative alla presente direttiva, ai documenti sulla resilienza a livello dell'Unione;

e) contribuire alla preparazione delle linee guida di cui all'articolo 7, paragrafo 3, e all'articolo 13, paragrafo 5, e, su richiesta, di ogni atto delegato o di esecuzione adottato ai sensi della presente direttiva;

f) analizzare le relazioni di sintesi di cui all'articolo 9, paragrafo 3, al fine di promuovere la condivisione delle migliori prassi sulle azioni intraprese ai sensi dell'articolo 15, paragrafo 3;

g) condividere migliori prassi in relazione alla notifica di incidenti di cui all'articolo 15;

h) discutere le relazioni di sintesi sulle missioni di consulenza e le lezioni apprese ai sensi dell'articolo 18, paragrafo 10;

i) scambiare informazioni e migliori prassi in materia di innovazione, ricerca e sviluppo in relazione alla resilienza dei soggetti critici ai sensi della presente direttiva;

j) se del caso, scambiare informazioni su questioni relative alla resilienza dei soggetti critici con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione.

4. Entro il 17 gennaio 2025 e in seguito ogni due anni, il gruppo per la resilienza dei soggetti critici stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti. Tale programma di lavoro è coerente con le prescrizioni e gli obiettivi della presente direttiva.

5. Il gruppo per la resilienza dei soggetti critici si riunisce periodicamente, e in ogni caso almeno una volta all'anno, con il gruppo di cooperazione istituito a norma della direttiva (UE) 2022/2555 al fine di promuovere e agevolare la cooperazione strategica e lo scambio di informazioni.

6. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo per la resilienza dei soggetti critici, conformemente all'articolo 1, paragrafo 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 24, paragrafo 2.

7. Entro il 17 gennaio 2027, e successivamente quando necessario e almeno ogni quattro anni, la Commissione trasmette al gruppo per la resilienza dei soggetti critici una relazione di sintesi sulle informazioni fornite dagli Stati membri ai sensi dell'articolo 4, paragrafo 3, e dell'articolo 5, paragrafo 4.

Articolo 20

Sostegno della Commissione alle autorità competenti e ai soggetti critici

1. La Commissione sostiene, se del caso, gli Stati membri e i soggetti critici nell'adempimento dei loro obblighi ai sensi della presente direttiva. Essa prepara una rassegna, a livello dell'Unione, dei rischi transfrontalieri e intersettoriali per la fornitura dei servizi essenziali, organizza le missioni di consulenza di cui all'articolo 13, paragrafo 4, e all'articolo 18 e agevola lo scambio di informazioni fra gli Stati membri ed esperti in tutta l'Unione.

2. La Commissione integra le attività degli Stati membri di cui all'articolo 10 sviluppando migliori prassi, materiali e metodologie di orientamento, così come attività di formazione ed esercitazioni transfrontaliere per testare la resilienza dei soggetti critici.

3. La Commissione informa gli Stati membri in merito alle risorse finanziarie a disposizione degli Stati membri a livello di Unione per rafforzare la resilienza dei soggetti critici.

CAPO VI

VIGILANZA ED ESECUZIONE

Articolo 21

Vigilanza ed esecuzione

1. Per valutare l'adempimento degli obblighi stabiliti dalla presente direttiva da parte dei soggetti individuati come soggetti critici ai sensi dell'articolo 6, paragrafo 1 dagli Stati membri, gli Stati membri provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi per:

a) effettuare ispezioni in loco dell'infrastruttura critica e dei siti utilizzati dal soggetto critico per fornire i suoi servizi essenziali, e vigilare da remoto sulle misure adottate dai soggetti critici conformemente all'articolo 13;

b) svolgere o disporre controlli nei confronti dei soggetti critici.

2. Gli Stati membri provvedono affinché le autorità competenti abbiano i poteri e i mezzi per richiedere, qualora necessario per lo svolgimento dei loro compiti ai sensi della presente direttiva, che i soggetti di cui alla direttiva (UE) 2022/2555 che sono stati individuati come soggetti critici ai sensi della presente direttiva forniscano, entro un ragionevole periodo di tempo stabilito da dette autorità:

a) le informazioni necessarie per valutare se le misure adottate da tali soggetti per garantire la loro resilienza soddisfino i requisiti stabiliti all'articolo 13;

b) la prova dell'effettiva attuazione di tali misure, inclusi i risultati di un controllo svolto da un revisore indipendente e qualificato, selezionato da tale soggetto, ed effettuato a spese di questo.

Quando richiede tali informazioni l'autorità competente indica lo scopo della richiesta specificando il tipo di informazioni da fornire.

3. Fatta salva la possibilità di irrogare sanzioni ai sensi dell'articolo 22, le autorità competenti possono esigere, a seguito delle azioni di vigilanza di cui al paragrafo 1 del presente articolo o della valutazione delle informazioni di cui al paragrafo 2 del presente articolo, che i soggetti critici interessati adottino entro un ragionevole periodo di tempo da esse stabilito le misure necessarie e proporzionate per porre rimedio a qualsiasi violazione individuata della presente direttiva e forniscano loro informazioni sulle misure adottate. Tali provvedimenti tengono conto, in particolare, della gravità della violazione.

4. Gli Stati membri provvedono affinché i poteri di cui ai paragrafi 1, 2 e 3 possano essere esercitati solo fatte salve le opportune garanzie. Deve essere garantito, in particolare, che tali poteri siano esercitati in modo obiettivo, trasparente e proporzionato e che siano debitamente tutelati i diritti e gli interessi legittimi, quali la protezione dei segreti commerciali e aziendali, dei soggetti critici interessati, inclusi il diritto al contraddittorio, i diritti della difesa e il diritto a un ricorso effettivo dinanzi a un giudice indipendente.

5. Gli Stati membri provvedono affinché, quando un'autorità competente ai sensi della presente direttiva valuta il rispetto degli obblighi da parte di un soggetto critico ai sensi del presente articolo, tale autorità competente informi le autorità competenti degli Stati membri interessati ai sensi della direttiva (UE) 2022/2555 A tale fine, gli Stati membri provvedono affinché le autorità competenti ai sensi della presente direttiva possano chiedere alle autorità competenti ai sensi della direttiva (UE) 2022/2555 di esercitare i propri poteri di vigilanza ed esecuzione nei confronti di un soggetto ai sensi di tale direttiva individuato come soggetto critico ai sensi della presente direttiva. A tal fine, gli Stati membri provvedono affinché le autorità competenti ai sensi della presente direttiva cooperino e scambino informazioni con tali autorità competenti ai sensi della direttiva (UE) 2022/2555

Articolo 22

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle misure nazionali adottate ai sensi della presente direttiva e prendono tutte le misure necessarie per assicurarne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive. Gli Stati membri notificano tali disposizioni alla Commissione al più tardi entro il 17 ottobre 2024, e provvedono poi a darle immediata notifica delle eventuali modifiche successive.

CAPO VII

ATTI DELEGATI E ATTI DI ESECUZIONE

Articolo 23

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 5, paragrafo 1, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 16 gennaio 2023.

3. La delega di potere di cui all'articolo 5, paragrafo 1, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta Ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 5, paragrafo 1, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 24

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

CAPO VIII

DISPOSIZIONI FINALI

Articolo 25

Relazioni e riesame

Entro il 17 luglio 2027, la Commissione presenta al Parlamento europeo e al Consiglio una relazione in cui valuta in quale misura ciascuno Stato membro abbia adottato le misure necessarie per conformarsi alla presente direttiva.

La Commissione riesamina periodicamente il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. Tale relazione valuta in particolare il valore aggiunto della presente direttiva, il suo impatto nel garantire la resilienza dei soggetti critici, e se l'allegato della presente direttiva debba essere modificato. La Commissione presenta la prima di tali relazioni entro il 17 giugno 2029. Al fine della relazione ai sensi del presente articolo, la Commissione tiene conto dei pertinenti documenti del gruppo per la resilienza dei soggetti critici.

Articolo 26

Recepimento

1. Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione.

Gli Stati membri applicano tali misure a decorrere dal 18 ottobre 2024.

2. Le misure di cui al paragrafo 1 adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 27

Abrogazione della direttiva 2008/114/CE

La direttiva 2008/114/CE è abrogata a decorrere dal 18 ottobre 2024.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva.

Articolo 28

Entrata in vigore

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

Articolo 29

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK

ALLEGATO

SETTORI, SOTTOSETTORI E CATEGORIE DI SOGGETTI

Settori	Sottosettori	Categorie di soggetti
1. Energia	a) Energia elettrica	— Imprese elettriche quali definite all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio ([1]) che svolgono l'attività di «fornitura» quali definite all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designati quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio ([2])
		— Partecipanti al mercato quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59), della direttiva (UE) 2019/944
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio ([3])
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio ([4])

Settori	Sottosettori	Categorie di soggetti
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio ([5])
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([6]), aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([7]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([8])

Settori	Sottosettori	Categorie di soggetti
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([9])
		— Imprese ferroviarie quali definite all'articolo 3, punto 1), della direttiva 2012/34/UE e operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite all'allegato I del regolamento (CE) n. 725/2004, escluse le singole navi gestite da tali compagnie
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE, compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([10])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione ([11]) responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([12])
	e) Trasporto pubblico	— Operatori di servizio pubblico quali definiti all'articolo 2, lettera d), del regolamento (CE) n. 1370/2007 del Parlamento europeo e del Consiglio ([13])
3. Settore bancario		— Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013
4. Infrastrutture dei mercati finanziari		— Gestori di sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012

Settori	Sottosettori	Categorie di soggetti
5. Salute		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([14])
		— Laboratori di riferimento dell'UE di cui all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio ([15])
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ([16])
		— Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2
		— Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica («elenco dei dispositivi critici per l'emergenza di sanità pubblica») ai sensi dell'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio ([17])
		— Soggetti titolari di un'autorizzazione di distribuzione di cui all'articolo 79 della direttiva 2001/83/CE
6. Acqua potabile		— Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1), lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio ([18]), esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		— Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, acque reflue domestiche o acque reflue industriali quali definite all'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio ([19]) escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, acque reflue domestiche e acque reflue industriali è una parte non essenziale della loro attività generale

Settori	Sottosettori	Categorie di soggetti
8. Infrastrutture digitali		— Fornitori di punti di interscambio Internet quali definiti all'articolo 6, punto 18), della direttiva (UE) 2022/2555
		— Fornitori di servizi DNS quali definiti all'articolo 6, punto 20), della direttiva (UE) 2022/2555, esclusi gli operatori dei server dei nomi radice
		— Registri dei nomi di dominio di primo livello quali definiti all'articolo 6, punto 21), della direttiva (UE) 2022/2555
		— Fornitori di servizi di cloud computing quali definiti all'articolo 6, punto 30), della direttiva (UE) 2022/2555
		— Fornitori di servizi di data center quali definiti all'articolo 6, punto 31), della direttiva (UE) 2022/2555
		— Fornitori di reti di distribuzione dei contenuti (content delivery network) quali definiti all'articolo 6, punto 32), della direttiva (UE) 2022/2555
		— Prestatori di servizi fiduciari quali definiti all'articolo 3, punto 19), del regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio ([20])
		— Fornitori di reti pubbliche di comunicazione elettronica quali definite all'articolo 2, punto 8), della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio ([21])
		— Fornitori di servizi di comunicazione elettronica ai sensi dell'articolo 2, punto 4), della direttiva (UE) 2018/1972 nella misura in cui tali servizi siano accessibili al pubblico
9. Enti della pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali come definiti da Stati membri conformemente al diritto nazionale
10. Spazio		— Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica quali definite all'articolo 2, punto 8), della direttiva (UE) 2018/1972

Settori	Sottosettori	Categorie di soggetti
11. Produzione, trasformazione e distribuzione di alimenti		— Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio ([22]) impegnate esclusivamente nella logistica e nella distribuzione all'ingrosso nonché nella produzione e trasformazione industriale su larga scala

([1]) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).
([2]) Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).
([3]) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).
([4]) Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).
([5]) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
([6]) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
([7]) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
([8]) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
([9]) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
([10]) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10).
([11]) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
([12]) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
([13]) Regolamento (CE) n. 1370/2007 del Parlamento europeo e del Consiglio, del 23 ottobre 2007, relativo ai servizi pubblici di trasporto di passeggeri su strada e per ferrovia e che abroga i regolamenti del Consiglio (CEE) n. 1191/69 e (CEE) n. 1107/70 (GU L 315 del 3.12.2007, pag. 1).
([14]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).
([15]) Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).
([16]) Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).
([17]) Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio, del 25 gennaio 2022, relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici (GU L 20 del 31.1.2022, pag. 1).
([18]) Direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, del 16 dicembre 2020, concernente la qualità delle acque destinate al consumo umano (GU L 435 del 23.12.2020, pag. 1).
([19]) Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).
([20]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).
([21]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).
([22]) Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 dell'1.2.2002, pag. 1).

ISSN 1977-0707 (edizione elettronica)
ISSN 1725-258X (edizione cartacea)

Ufficio delle pubblicazioni
dell'Unione europea
L-2985 Lussemburgo
LUSSEMBURGO

IT