2025/38

15.1.2025

REGOLAMENTO (UE) 2025/38 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 19 dicembre 2024

che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 173, paragrafo 3, e l'articolo 322, paragrafo 1, lettera a),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Corte dei conti ([1]),

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

visto il parere del Comitato delle regioni ([3]),

deliberando secondo la procedura legislativa ordinaria ([4]),

considerando quanto segue:

(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica e della società, date l'interconnessione e l'interdipendenza crescenti delle pubbliche amministrazioni, delle imprese e dei cittadini degli Stati membri a livello transettoriale e transfrontaliero, il che ha introdotto al tempo stesso possibili vulnerabilità.

(2) L'entità, la frequenza el'impatto degli incidenti di cibersicurezza, compresi gli attacchi alle catene di approvvigionamento a fini di ciberspionaggio, di ransomware o di perturbazione, sono in crescita a livello dell'Unione e su scala mondiale. Tali incidenti rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi, In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti di cibersicurezza su vasta scala capaci di provocare perturbazioni o danni significativi a infrastrutture critiche, richiede una maggiore preparazione del quadro di cibersicurezza dell'Unione. Tale minaccia va oltre la guerra di aggressione della Russia nei confronti dell'Ucraina ed è destinata a persistere, data la molteplicità di soggetti coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici, dal momento che gli attacchi informatici sono spesso diretti a infrastrutture e servizi pubblici locali, regionali o nazionali, e le autorità locali sono particolarmente vulnerabili, anche a causa delle loro risorse limitate. Possono altresì ostacolare lo svolgimento di attività economiche, anche in settori altamente critici o in altri settori critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni alle economie e ai sistemi democratici dell'Unione, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali. Inoltre, gli incidenti di cibersicurezza sono imprevedibili, in quanto spesso si verificano ed evolvono rapidamente, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi. È importante che vi sia una stretta cooperazione tra il settore pubblico, il settore privato, il mondo accademico, la società civile e i media.

(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitale e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa. È necessario accrescere la resilienza dei cittadini, delle imprese, comprese le microimprese, le piccole e medie imprese e le start-up, e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce informatiche, che possono avere conseguenze devastanti a livello sociale ed economico. Occorre quindi investire in infrastrutture e servizi e creare capacità per sviluppare competenze in materia di cibersicurezza che permettano di velocizzare il

([1]) Parere del 18 aprile 2023 (non ancora pubblicato nella Gazzetta Ufficiale)
([2]) GU C 349 del 29.9.2023, pag. 167.
([3]) GU C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
([4]) Posizione del Parlamento europeo del 24 aprile 2024 (non ancora pubblicato nella Gazzetta Ufficiale) e decisione del Consiglio del 2 dicembre 2024.

rilevamento delle minacce e degli incidenti informatici e di assicurare una risposta più rapida. Inoltre, gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, nonché di assistenza nella ripresa iniziale dagli stessi. Basandosi sulle strutture esistenti e in stretta cooperazione con le stesse, l'Unione dovrebbe inoltre accrescere le sue capacità in tali settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti informatici.

(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi, in particolare il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([5]), le direttive 2013/40/UE ([6]) e (UE) 2022/2555 ([7]) del Parlamento europeo e del Consiglio e la raccomandazione (UE) 2017/1584 della Commissione ([8]). Inoltre, la raccomandazione del Consiglio dell'8 dicembre 2022 su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure e a cooperare tra loro, con la Commissione e le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

(5) I crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono il rafforzamento della solidarietà a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti informatici, nonché la preparazione e la risposta agli stessi, come pure la ripresa dai medesimi, in particolare rafforzando le capacità delle strutture esistenti. Inoltre, le conclusioni del Consiglio del 23 maggio 2022 su una posizione dell'UE in materia di deterrenza informatica hanno invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

(6) La comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 10 novembre 2022 al Parlamento europeo e al Consiglio sulla politica di ciberdifesa dell'UE ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi di rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la mobilitazione di un'infrastruttura unionale dei centri operativi di sicurezza (Security Operation Centres — SOC), sostenere la costituzione graduale di una riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE.

(7) Occorre rafforzare il rilevamento e la conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e le capacità degli Stati membri e dell'Unione di prevenire gli incidenti di cibersicurezza significativi e gli incidenti di cibersicurezza su vasta scala e di rispondervi. Di conseguenza si dovrebbe istituire una rete paneuropea di poli informatici (il sistema europeo di allerta per la cibersicurezza) per sviluppare capacità coordinate in materia di rilevamento e conoscenza situazionale, rafforzando le capacità dell'Unione in materia di rilevamento delle minacce e di condivisione delle informazioni; si dovrebbe istituire un meccanismo per le emergenze di cibersicurezza, al fine di sostenere gli Stati membri, su loro richiesta, nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, nell'attenuarne l'effetto e nell'avviare la ripresa dagli stessi, e di sostenere altri utenti nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e si dovrebbe istituire un meccanismo europeo di riesame degli incidenti di cibersicurezza per riesaminare e valutare specifici incidenti di cibersicurezza significativi o incidenti di cibersicurezza su vasta scala. Le azioni intraprese a norma del presente regolamento dovrebbero essere realizzate nel debito rispetto delle competenze degli Stati membri e dovrebbero integrare e non duplicare le attività svolte dalla rete di CSIRT, dalla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) o dal gruppo di cooperazione (gruppo di cooperazione NIS), tutti istituiti a norma della direttiva (UE) 2022/2555. Tali azioni non pregiudicano gli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea (TFUE).

([5]) 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).

([6]) 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).

([7]) 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 (GU L 333 del 27.12.2022, pag. 80).

([8]) 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).

(8) Per conseguire questi obiettivi occorre modificare il regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio ([9]) in alcuni settori. In particolare il presente regolamento dovrebbe modificare il regolamento (UE) 2021/694 aggiungendo nuovi obiettivi operativi relativi al sistema europeo di allerta per la cibersicurezza e al meccanismo per le emergenze di cibersicurezza nell'ambito dell'obiettivo specifico 3 del programma Europa digitale, che mira a garantire la resilienza, l'integrità e l'affidabilità del mercato unico digitale, a rafforzare le capacità di monitoraggio delle minacce e degli attacchi informatici e di risposta agli stessi, nonché a rafforzare la cooperazione e il coordinamento transfrontalieri in materia di cibersicurezza. Il sistema europeo di allerta per la cibersicurezza potrebbe svolgere un ruolo importante aiutando gli Stati membri ad anticipare le minacce informatiche e a proteggersi dalle stesse, e la riserva dell'UE per la cibersicurezza potrebbe svolgere un ruolo importante aiutando gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i paesi terzi associati al programma Europa digitale a rispondere agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala, e ad attenuarne l'effetto. Tale effetto potrebbe includere danni materiali o immateriali considerevoli e gravi rischi di pubblica sicurezza. Alla luce dei ruoli specifici che il sistema europeo di allerta per la cibersicurezza e la riserva dell'UE per la cibersicurezza potrebbero svolgere, il presente regolamento dovrebbe modificare il regolamento (UE) 2021/694 per quanto riguarda la partecipazione dei soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi, nel caso in cui vi sia un rischio reale che gli strumenti, le infrastrutture e i servizi necessari e sufficienti, o le tecnologie, le competenze e le capacità necessarie e sufficienti, non siano disponibili nell'Unione e i vantaggi derivanti dall'inclusione di tali soggetti siano superiori ai rischi per la sicurezza. È opportuno stabilire le condizioni specifiche in base alle quali può essere concesso il sostegno finanziario per le azioni volte ad attuare il sistema europeo di allerta per la cibersicurezza e la riserva dell'UE per la cibersicurezza e definire i meccanismi di governance e di coordinamento necessari per raggiungere gli obiettivi previsti. Altre modifiche del regolamento (UE) 2021/694 dovrebbero includere descrizioni delle azioni proposte nell'ambito dei nuovi obiettivi operativi, nonché indicatori misurabili per monitorarne l'attuazione di questi ultimi.

(9) Per rafforzare la risposta dell'Unione alle minacce e agli incidenti informatici, è essenziale la cooperazione con le istituzioni internazionali e con i partner internazionali di fiducia che condividono gli stessi principi. In tale contesto, per partner internazionali di fiducia che condividono gli stessi principi si dovrebbero intendere i paesi che condividono i principi che hanno informato la creazione dell'Unione, vale a dire la democrazia, lo Stato di diritto, l'universalità e indivisibilità dei diritti umani e delle libertà fondamentali, il rispetto della dignità umana, i principi di uguaglianza e solidarietà e il rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale, e che non pregiudicano gli interessi essenziali dell'Unione o dei suoi Stati membri in materia di sicurezza. Tale cooperazione potrebbe essere vantaggiosa anche per quanto riguarda le azioni intraprese a norma del presente regolamento, in particolare il sistema europeo di allerta per la cibersicurezza e la riserva dell'UE per la cibersicurezza. Il regolamento (UE) 2021/694 dovrebbe prevedere, a condizione che siano soddisfatte determinate condizioni di disponibilità e sicurezza, che le gare d'appalto per tali infrastrutture, strumenti e servizi potrebbero essere aperte a soggetti giuridici controllati da paesi terzi, a condizione che siano rispettati i requisiti di sicurezza. Nel valutare il rischio per la sicurezza derivante da tale apertura dell'appalto, è importante tenere conto dei principi e dei valori che l'Unione condivide con partner internazionali che condividono gli stessi principi, laddove tali principi siano connessi agli interessi essenziali dell'Unione in materia di sicurezza. Inoltre, quando tali requisiti di sicurezza sono considerati a norma del regolamento (UE) 2021/694, si potrebbe tenere conto di diversi elementi, quali la struttura societaria e il processo decisionale di un soggetto, la sicurezza dei dati e delle informazioni classificate o sensibili e la garanzia che i risultati dell'azione non siano soggetti a controlli o restrizioni da parte di paesi terzi non ammissibili.

(10) Il finanziamento delle azioni ai sensi del presente regolamento dovrebbe essere previsto dal regolamento (UE) 2021/694, che dovrebbe rimanere l'atto di base pertinente per le azioni di cui nell'obiettivo specifico 3 del programma Europa digitale. Le condizioni specifiche di partecipazione riguardanti ciascuna azione devono essere indicate nei programmi di lavoro, conformemente al regolamento (UE) 2021/694.

(11) Al presente regolamento si applicano le regole finanziarie orizzontali adottate dal Parlamento europeo e dal Consiglio in base all'articolo 322 TFUE. Tali regole sono stabilite nel regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio ([10]), definiscono in particolare le modalità relative alla formazione e all'esecuzione del bilancio dell'Unione e organizzano il controllo della responsabilità degli agenti finanziari. Le

([9]) Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240 (GU L 166 dell'11.5.2021, pag. 1).

([10]) Regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio, del 23 settembre 2024, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione (GU L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

regole adottate in base all'articolo 322 TFUE comprendono anche un regime generale di condizionalità per la protezione del bilancio dell'Unione istituito dal regolamento (UE, Euratom) 2020/2092 del Parlamento europeo e del Consiglio ([11]).

(12) Benché le misure di prevenzione e preparazione siano essenziali per rafforzare la resilienza dell'Unione nel far fronte a incidenti significativi di cibersicurezza, incidenti di cibersicurezza su vasta scala e incidenti di cibersicurezza equivalenti a incidenti su vasta scala, l'insorgenza, i tempi e la portata degli incidenti sono per loro natura imprevedibili. Le risorse finanziarie necessarie per garantire una risposta adeguata possono variare notevolmente da un anno all'altro e dovrebbero poter essere messe immediatamente a disposizione. Per conciliare il principio di bilancio della prevedibilità con la necessità di reagire rapidamente alle nuove esigenze è pertanto necessario adattare l'esecuzione finanziaria dei programmi di lavoro. Di conseguenza, è opportuno autorizzare il riporto degli stanziamenti inutilizzati, limitatamente all'anno successivo ed esclusivamente per la riserva dell'UE per la cibersicurezza e le azioni a sostegno dell'assistenza reciproca, in aggiunta al riporto degli stanziamenti autorizzati ai sensi dell'articolo 12, paragrafo 4, del regolamento (UE, Euratom) 2024/2509.

(13) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, la relativa risposta e la ripresa dagli stessi, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture. Un approccio proattivo all'individuazione, all'attenuazione e alla prevenzione delle minacce informatiche include maggiori capacità di rilevamento avanzate. Il sistema europeo di allerta per la cibersicurezza dovrebbe consistere in diversi poli informatici transfrontalieri interoperanti, ciascuno composto da tre o più poli informatici nazionali. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per la raccolta avanzata di dati e informazioni pertinenti, se del caso anonimizzati, e strumenti di analisi, migliorando le capacità di rilevamento e di gestione coordinate delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. Dovrebbe inoltre servire a migliorare la posizione in materia di deterrenza informatica, aumentando il rilevamento, l'aggregazione e l'analisi di dati e informazioni al fine di prevenire le minacce e gli incidenti informatici e quindi integrando e sostenendo i soggetti e le reti dell'Unione responsabili della gestione delle crisi informatiche nell'UE, in particolare EU-CyCLONe.

(14) La partecipazione al sistema europeo di allerta per la cibersicurezza è volontaria per gli Stati membri. Ogni Stato membro dovrebbe designare un unico soggetto a livello nazionale, incaricato di coordinare le attività di rilevamento delle minacce informatiche in tale Stato membro. Questi poli informatici nazionali dovrebbero fungere da punto di riferimento e porta di accesso a livello nazionale per la partecipazione al sistema europeo di allerta per la cibersicurezza e garantire che le informazioni sulle minacce informatiche provenienti da soggetti pubblici e privati siano condivise e raccolte a livello nazionale in modo efficace e semplificato. I poli informatici nazionali potrebbero rafforzare la cooperazione e la condivisione di informazioni tra soggetti pubblici e privati e sostenere inoltre lo scambio di dati e informazioni pertinenti con le comunità settoriali e intersettoriali pertinenti, compresi i centri di analisi e condivisione delle informazioni («ISAC») settoriali pertinenti. Una cooperazione stretta e coordinata tra soggetti pubblici e privati è fondamentale per rafforzare la resilienza informatica dell'Unione. Tale cooperazione è particolarmente utile nel contesto della condivisione di analisi sulle minacce informatiche al fine di migliorare la protezione informatica attiva. Nell'ambito di tale cooperazione e condivisione di informazioni, i poli informatici nazionali potrebbero richiedere e ricevere informazioni specifiche. Il presente regolamento non obbliga né autorizza tali poli informatici nazionali a dare attuazione a tali richieste. Se del caso e conformemente al diritto dell'Unione e nazionale, le informazioni richieste o ricevute potrebbero includere dati raccolti mediante telemetria, sensori e registrazioni di soggetti quali i fornitori di servizi di sicurezza gestiti, che operano in settori ad alta criticità o in altri settori critici all'interno di tale Stato membro, al fine di migliorare il rilevamento rapido di potenziali minacce e incidenti informatici in una fase precoce, migliorando in tal modo la conoscenza situazionale. Se il polo informatico nazionale non è l'autorità competente designata o istituita dallo Stato membro interessato a norma dell'articolo 8, paragrafo 1 della direttiva (UE) 2022/2555, è fondamentale che si coordini con tale autorità competente per quanto riguarda le richieste di tali dati e il loro ricevimento.

(15) Nell'ambito del sistema europeo di allerta per la cibersicurezza è opportuno istituire diversi poli informatici transfrontalieri. I poli informatici transfrontalieri dovrebbero riunire i poli informatici nazionali di almeno tre Stati membri per garantire che siano sfruttati appieno i vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei poli informatici transfrontalieri dovrebbe

([11]) Regolamento (UE, Euratom) 2020/2092 del Parlamento europeo e del Consiglio, del 16 dicembre 2020, relativo a un regime generale di condizionalità per la protezione del bilancio dell'Unione (GU L 433 I del 22.12.2020, pag. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce informatiche e di favorire l'elaborazione di analisi di alta qualità sulle minacce informatiche, in particolare mediante la condivisione di informazioni pertinenti, se del caso anonimizzati, in un contesto sicuro e di fiducia, provenienti da varie fonti, pubbliche o private, nonché tramite la condivisione e l'uso congiunto di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e prevenzione in un contesto sicuro e di fiducia. I poli informatici transfrontalieri dovrebbero garantire nuove capacità aggiuntive, basandosi sui SOC, sui CSIRT esistenti nonché su altri soggetti pertinenti, compresa la rete di CSIRT, e integrandoli.

(16) Uno Stato membro selezionato dal Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca istituito dal regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio ([12]) (ECCC) a seguito di un invito a manifestare interesse al fine di istituire un polo informatico nazionale o di rafforzarne le capacità dovrebbe acquistare gli strumenti, le infrastrutture o i servizi pertinenti congiuntamente all'ECCC. Tale Stato membro dovrebbe poter beneficiare di una sovvenzione per l'utilizzo degli strumenti, delle infrastrutture o dei servizi. Un consorzio ospitante composto da almeno tre Stati membri, selezionato dall'ECCC a seguito di un invito a manifestare interesse al fine di istituire un polo informatico transfrontaliero o di rafforzarne le capacità, dovrebbe acquistare gli strumenti, le infrastrutture o i servizi pertinenti congiuntamente con l'ECCC. Il consorzio ospitante dovrebbe poter beneficiare di una sovvenzione per l'utilizzo degli strumenti, delle infrastrutture o dei servizi. La procedura di appalto per l'acquisto degli strumenti, delle infrastrutture o dei servizi pertinenti dovrebbe essere realizzata congiuntamente dall'ECCC e dalle amministrazioni aggiudicatrici competenti degli Stati membri selezionati a seguito di tali inviti a manifestare interesse. Tale appalto dovrebbe essere conforme all'articolo 168, paragrafo 2, del regolamento (UE, Euratom) 2024/2509 e con il regolamento finanziario dell'ECCC. I soggetti privati non dovrebbero pertanto essere ammessi a partecipare agli inviti a manifestare interesse per l'acquisto di strumenti, infrastrutture e servizi congiuntamente con l'ECCC né a ricevere sovvenzioni per l'utilizzo di tali strumenti, infrastrutture o servizi. Tuttavia, gli Stati membri dovrebbero poter coinvolgere soggetti privati nell'istituzione, nel rafforzamento e nel funzionamento dei loro poli informatici nazionali e dei poli informatici transfrontalieri in altre forme che ritengono opportune, nel rispetto del diritto dell'Unione e nazionale. I soggetti privati potrebbero anche beneficiare di un finanziamento dell'Unione a norma del regolamento (UE) 2021/887 al fine di fornire sostegno ai poli informatici nazionali.

(17) Al fine di migliorare il rilevamento delle minacce informatiche e la conoscenza situazionale nell'Unione, uno Stato membro selezionato a seguito di un invito a manifestare interesse al fine di istituire un polo informatico nazionale o di rafforzarne le capacità dovrebbe impegnarsi a candidarsi per partecipare a un polo informatico transfrontaliero. Se uno Stato membro non partecipa a un polo informatico transfrontaliero entro due anni dalla data di acquisizione degli strumenti, delle infrastrutture o dei servizi o, se precedente, dalla data in cui riceve la sovvenzione, esso non dovrebbe essere ammesso a partecipare ad altre azioni di sostegno dell'Unione nel quadro del sistema europeo di allerta sulla cibersicurezza, volte a rafforzare le capacità del suo polo informatico nazionale. In tali casi, i soggetti degli Stati membri potrebbero ancora partecipare a inviti a presentare proposte su altri temi nell'ambito del programma Europa digitale o di altri programmi di finanziamento dell'Unione, compresi inviti a presentare proposte per il rilevamento delle minacce informatiche e la condivisione di informazioni, a condizione che tali soggetti soddisfino i criteri di ammissibilità stabiliti nei programmi.

(18) I CSIRT inoltre scambiano informazioni nell'ambito della rete di CSIRT conformemente a quanto disposto dalla direttiva (UE) 2022/2555. Il sistema europeo di allerta per la cibersicurezza dovrebbe costituire una nuova capacità complementare alla rete di CSIRT contribuendo allo sviluppo di una conoscenza situazionale dell'Unione che consenta il rafforzamento delle capacità della rete di CSIRT. I poli informatici transfrontalieri dovrebbero coordinarsi e cooperare strettamente con la rete di CSIRT. Essi dovrebbero agire mettendo in comune dati e condividendo informazioni pertinenti, se del caso anonimizzati, sulle minacce informatiche provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati e informazioni mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo alla sovranità tecnologica dell'Unione, alla sua autonomia strategica aperta, alla sua competitività e resilienza, nonché allo sviluppo delle capacità dell'Unione.

(19) I poli informatici transfrontalieri dovrebbero fungere da punto centrale in grado di consentire un'ampia condivisione di dati pertinenti e di analisi delle minacce informatiche e permettere la diffusione di informazioni sulle minacce tra più portatori di interessi di diversa natura, quali le squadre di pronto intervento informatico (Computer Emergency Response Teams — CERT), i CSIRT, gli ISAC e gli operatori di infrastrutture critiche. I membri di un consorzio ospitante dovrebbero specificare nell'accordo di consorzio le informazioni pertinenti da condividere tra i partecipanti al polo informatico transfrontaliero interessato. Le informazioni scambiate tra i partecipanti a un polo informatico transfrontaliero potrebbero includere, ad esempio, dati provenienti da reti e sensori, feed di analisi delle minacce, indicatori di compromissione e informazioni contestualizzate su incidenti, minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di

([12]) Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (GU L 202 dell'8.6.2021, pag. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

cibersicurezza e raccomandazioni relative alla configurazione degli strumenti di cibersicurezza per rilevare gli attacchi informatici. I poli informatici transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione tra loro. Tali accordi di cooperazione dovrebbero specificare, in particolare, i principi di condivisione delle informazioni e l'interoperabilità. Le loro clausole relative all'interoperabilità, in particolare i formati e i protocolli per la condivisione delle informazioni, dovrebbero ispirarsi agli orientamenti di interoperabilità emanati dall'Agenzia dell'Unione europea per la cibersicurezza istituita dal regolamento (UE) 2019/881 (ENISA) e prenderli pertanto come punto di partenza. Tali orientamenti dovrebbero essere pubblicati rapidamente per garantire che possano essere presi in considerazione dai poli informatici transfrontalieri in una fase precoce. Essi dovrebbero tenere conto delle norme internazionali, e delle migliori pratiche e del funzionamento dei diversi poli informatici transfrontalieri.

(20) I poli informatici transfrontalieri e la rete di CSIRT dovrebbero cooperare strettamente per garantire sinergie e la complementarità delle attività. A tal fine, dovrebbero concordare modalità procedurali in materia di cooperazione e condivisione delle informazioni pertinenti. Ciò potrebbe includere la condivisione di informazioni pertinenti sulle minacce informatiche e sugli incidenti di cibersicurezza significativi e la garanzia che le esperienze derivanti dall'uso di strumenti all'avanguardia, in particolare l'intelligenza artificiale e le tecnologie di analisi dei dati, nell'ambito dei poli informatici transfrontalieri, siano condivise con la rete di CSIRT.

(21) La condivisione della conoscenza situazionale tra le autorità competenti è un prerequisito indispensabile per la preparazione e il coordinamento a livello dell'Unione in caso di incidenti di cibersicurezza significativi e incidenti di cibersicurezza su vasta scala. La direttiva (UE) 2022/2555 ha istituito EU-CyCLONe 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. La direttiva (UE) 2022/2555 ha anche istituito la rete di CSIRT per promuovere una cooperazione operativa rapida ed efficace tra tutti gli Stati membri. Per garantire la conoscenza situazionale e rafforzare la solidarietà, nelle situazioni in cui ottengono informazioni relative a un incidente di cibersicurezza potenziale o in corso su vasta scala, i poli informatici transfrontalieri dovrebbero fornire informazioni pertinenti alla rete di CSIRT e informare, per mezzo di un allarme rapido, EU-CyCLONe. In particolare, a seconda della situazione, le informazioni da condividere potrebbero includere informazioni tecniche, informazioni sulla natura e sulle motivazioni dell'autore di un attacco informatico o di un potenziale autore nonché informazioni non tecniche di livello superiore su un incidente di cibersicurezza potenziale o in corso su vasta scala. In tale contesto è opportuno prestare la dovuta attenzione al principio della necessità di conoscere e alla natura potenzialmente sensibile delle informazioni condivise. La direttiva (UE) 2022/2555 ribadisce altresì le responsabilità della Commissione nell'ambito del meccanismo unionale di protezione civile (Union Civil Protection Mechanism — UCPM) istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([13]), nonché la sua responsabilità per quanto riguarda la fornitura di relazioni analitiche per i dispositivi integrati dell'UE per la risposta politica alle crisi («dispositivi IPCR») ai sensi della decisione di esecuzione (UE) 2018/1993 del Consiglio ([14]). Quando i poli informatici transfrontalieri condividono con EU-CyCLONe e la rete di CSIRT informazioni pertinenti e allarmi rapidi relativi a un incidente di cibersicurezza potenziale o in corso su vasta scala, è indispensabile che tali informazioni siano condivise attraverso tali reti con le autorità degli Stati membri e con la Commissione. A tale riguardo, la direttiva (UE) 2022/2555 prevede che l'obiettivo di EU-CyCLONe è 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. I compiti di EU-CyCLONe includono lo sviluppo di una conoscenza situazionale condivisa per quanto riguarda tali incidenti e crisi. È di fondamentale importanza che EU-CyCLONe garantisca, in linea con tale obiettivo e con i suoi compiti, che tali informazioni siano immediatamente condivise con i rappresentanti degli Stati membri interessati e alla Commissione. A tal fine, è essenziale che il regolamento interno di EU-CyCLONe includa disposizioni appropriate.

(22) I soggetti che partecipano al sistema europeo di allerta per la cibersicurezza dovrebbero garantire un elevato livello di interoperabilità tra di loro, che riguardi anche, a seconda dei casi, il formato dei dati, la tassonomia e gli strumenti di gestione e di analisi dei dati. Essi dovrebbero inoltre assicurare canali di comunicazione sicuri, un livello minimo di sicurezza del livello applicazioni, un quadro operativo della conoscenza situazionale e indicatori. L'adozione di una tassonomia comune e la definizione di un modello per le relazioni sulla situazione al fine di descrivere le cause delle minacce informatiche rilevate e dei rischi dovrebbero tenere conto dei lavori già realizzati in materia di notifica degli incidenti nel contesto dell'attuazione della direttiva (UE) 2022/2555.

([13]) 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

([14]) 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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(23) Per consentire lo scambio di dati e informazioni pertinenti sulle minacce informatiche provenienti da varie fonti, su vasta scala, in un contesto sicuro e di fiducia, i soggetti che partecipano al sistema europeo di allerta per la cibersicurezza dovrebbero essere dotati di strumenti, apparecchiature e infrastrutture all'avanguardia, altamente sicuri, nonché di personale qualificato. Ciò dovrebbe consentire di migliorare le capacità collettive di rilevamento e di avvertire tempestivamente le autorità e i soggetti competenti, in particolare utilizzando le più recenti tecnologie di intelligenza artificiale e di analisi dei dati.

(24) Mediante la raccolta, l'analisi, la condivisione e lo scambio di dati e informazioni pertinenti, il sistema europeo di allerta per la cibersicurezza dovrebbe rafforzare la sovranità tecnologica dell'Unione, la sua autonomia strategica nel campo della cibersicurezza, nonché la sua competitività e resilienza. La condivisione di dati selezionati di alta qualità potrebbe inoltre contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati. La sorveglianza umana e quindi una forza lavoro qualificata rimangono essenziali per la condivisione efficace di dati di alta qualità.

(25) Sebbene il sistema europeo di allerta per la cibersicurezza sia un progetto civile, la comunità della ciberdifesa potrebbe trarre beneficio dalle maggiori capacità di rilevamento e di conoscenza situazionale sviluppate nel settore civile per la protezione delle infrastrutture critiche.

(26) La condivisione delle informazioni tra i partecipanti al sistema europeo di allerta per la cibersicurezza dovrebbe essere conforme alle prescrizioni giuridiche esistenti e in particolare al diritto nazionale e dell'Unione in materia di protezione dei dati, nonché alle norme dell'Unione sulla concorrenza che disciplinano lo scambio di informazioni. Il destinatario delle informazioni dovrebbe attuare, nella misura in cui il trattamento dei dati personali sia necessario, misure tecniche e organizzative a salvaguardia dei diritti e delle libertà degli interessati, distruggere i dati non appena non sono più necessari per la finalità dichiarata e comunicarne la distruzione al soggetto che li ha resi disponibili.

(27) Preservare la riservatezza e la sicurezza delle informazioni è di fondamentale importanza per tutti e tre i pilastri del presente regolamento, che si tratti di incoraggiare la condivisione o lo scambio di informazioni nel contesto del sistema europeo di allerta per la cibersicurezza, di preservare gli interessi dei soggetti che chiedono sostegno a titolo del meccanismo per le emergenze di cibersicurezza o di garantire che le relazioni nell'ambito del meccanismo europeo di riesame degli incidenti di cibersicurezza possano trarre insegnamenti utili senza incidere negativamente sui soggetti interessati dagli incidenti. La partecipazione degli Stati membri e dei soggetti a tali meccanismi dipende dai rapporti di fiducia tra le loro componenti. Qualora le informazioni siano riservate ai sensi delle norme dell'Unione o nazionali, la loro condivisione o il loro scambio a norma del presente regolamento dovrebbero essere limitati alle informazioni pertinenti e commisurate a tali scopi. Tale condivisione o scambio dovrebbe inoltre tutelare la riservatezza di tali informazioni e proteggere la sicurezza e gli interessi commerciali dei soggetti interessati. La condivisione o lo scambio di informazioni ai sensi del presente regolamento potrebbe avvenire per mezzo di accordi di non divulgazione o di orientamenti sulla diffusione delle informazioni, come il protocollo del semaforo (Traffic Light Protocol — TLP). Il TLP deve essere inteso come strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. Esso è utilizzato in quasi tutti i CSIRT e in alcuni ISAC. Oltre a tali requisiti generali, per quanto riguarda il sistema europeo di allerta per la cibersicurezza, gli accordi di consorzio ospitante dovrebbero stabilire norme specifiche relative alle condizioni per la condivisione di informazioni all'interno del polo informatico transfrontaliero interessato. Tali accordi potrebbero, in particolare, imporre che le informazioni siano scambiate unicamente in conformità del diritto dell'Unione e nazionale.

(28) Per quanto riguarda la mobilitazione della riserva dell'UE per la cibersicurezza, sono necessarie norme specifiche in materia di riservatezza. Il sostegno sarà richiesto, valutato e fornito in un contesto di crisi e in relazione a soggetti che operano in settori sensibili. Affinché la riserva dell'UE per la cibersicurezza funzioni efficacemente, è essenziale che gli utenti e i soggetti possano condividere e fornire un accesso immediato a tutte le informazioni necessarie in modo che ciascun soggetto possa svolgere il proprio ruolo nella valutazione delle richieste e nella mobilitazione del sostegno. Di conseguenza, il presente regolamento dovrebbe prevedere che tutte queste informazioni siano utilizzate o condivise solo se ciò è necessario per il funzionamento della riserva dell'UE per la cibersicurezza, e che le informazioni riservate o classificate ai sensi del diritto dell'Unione e nazionale siano utilizzate e condivise solo conformemente a tale diritto. Inoltre, gli utenti dovrebbero sempre essere in grado, se del caso, di utilizzare protocolli di condivisione delle informazioni come il protocollo TLP per specificare ulteriormente le limitazioni. Benché gli utenti dispongano di un margine di discrezionalità al riguardo, è importante che, nell'applicare tali limitazioni, essi tengano conto delle possibili conseguenze, in particolare per quanto riguarda il ritardo nella valutazione o nella fornitura dei servizi richiesti. Al fine di disporre di una riserva europea per la cibersicurezza efficiente, è importante che l'amministrazione aggiudicatrice chiarisca tali conseguenze all'utente prima che questo

presenti una richiesta. Tali garanzie sono limitate alla richiesta e alla fornitura di servizi della riserva europea per la cibersicurezza e non incidono sullo scambio di informazioni in altri contesti, ad esempio negli appalti relativi alla riserva europea per la cibersicurezza.

(29) Alla luce dell'aumento dei rischi e del numero di incidenti che colpiscono gli Stati membri, occorre istituire uno strumento di sostegno alle crisi, ovvero il meccanismo per le emergenza di cibersicurezza, per migliorare la resilienza dell'Unione agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta agli incidenti e il ripristino immediato dei servizi essenziali. Poiché la piena ripresa da un incidente è un processo globale di ripristino del funzionamento del soggetto interessato dall'incidente allo Stato precedente all'incidente e potrebbe essere un processo lungo che comporta costi significativi, il sostegno della riserva dell'UE per la cibersicurezza dovrebbe essere limitato alla fase iniziale del processo di recupero, che porti al ripristino delle funzionalità di base dei sistemi. Il meccanismo per le emergenze di cibersicurezza dovrebbe consentire una rapida ed efficace mobilitazione dell'assistenza in circostanze definite e nel rispetto di condizioni ben precise, e permettere un monitoraggio e una valutazione accurati delle modalità di utilizzo delle risorse. Sebbene agli Stati membri spetti la responsabilità primaria della prevenzione degli incidenti e delle crisi, nonché della preparazione e della risposta agli stessi, il meccanismo per le emergenze di cibersicurezza promuove la solidarietà tra gli Stati membri conformemente all'articolo 3, paragrafo 3, del trattato sull'Unione europea (TUE).

(30) Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire un sostegno agli Stati membri, integrando le loro misure e le loro risorse nonché altre opzioni di sostegno esistenti in caso di risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala e di ripresa iniziale dagli stessi, come i servizi forniti dall'ENISA conformemente al suo mandato, la risposta coordinata e l'assistenza della rete di CSIRT, il sostegno a strategie di attenuazione offerto da EU-CyCLONe, nonché l'assistenza reciproca tra gli Stati membri, anche nel contesto dell'articolo 42, paragrafo 7, TUE, e dei gruppi di risposta rapida agli incidenti informatici della cooperazione strutturata permanente (PESCO) istituiti a norma della decisione (PESC) 2017/2315 del Consiglio ([15]). Tale meccanismo dovrebbe rispondere alla necessità di garantire la disponibilità di mezzi specializzati per sostenere la preparazione e la risposta agli incidenti di cibersicurezza e la ripresa dagli stessi in tutta l'Unione e nei paesi terzi associati al programma Europa digitale.

(31) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare la direttiva (UE) 2022/2555, il meccanismo unionale di protezione civile istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([16]), i dispositivi IPCR e la raccomandazione 2017/1584 della Commissione ([17]). Il sostegno fornito nell'ambito del meccanismo per le emergenze di cibersicurezza può integrare l'assistenza fornita nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune, anche mediante i gruppi di risposta rapida agli incidenti informatici, tenendo conto della natura civile del meccanismo per le emergenze di cibersicurezza. Il sostegno fornito nell'ambito del meccanismo per le emergenze di cibersicurezza può integrare le azioni attuate nel contesto dell'articolo 42, paragrafo 7, TUE, compresa l'assistenza fornita da uno Stato membro a un altro Stato membro, o far parte della risposta congiunta tra l'Unione e gli Stati membri o nelle situazioni definite all'articolo 222 TFUE. L'attuazione del presente regolamento dovrebbe inoltre essere coordinato, laddove opportuno, con l'attuazione delle misure del pacchetto di strumenti della diplomazia informatica.

(32) L'assistenza fornita ai sensi del presente regolamento dovrebbe sostenere e integrare le azioni intraprese dagli Stati membri a livello nazionale. A tal fine occorre garantire stretta collaborazione e consultazione tra la Commissione, l'ENISA, gli Stati membri e, ove opportuno, l'ECCC. Nel richiedere un sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza, gli Stati membri dovrebbero fornire informazioni pertinenti che ne giustifichino la necessità.

(33) Secondo quanto disposto dalla direttiva (UE) 2022/2555, gli Stati membri sono tenuti a designare o istituire una o più autorità di gestione delle crisi informatiche e a garantire che tali autorità dispongano di risorse adeguate per svolgere i loro compiti in modo efficace ed efficiente. La direttiva impone inoltre gli Stati membri di individuare le capacità, le risorse e le procedure da poter mobilitare in caso di crisi, nonché di adottare un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, in cui siano definiti gli obiettivi e le modalità di gestione degli stessi. Gli Stati membri sono altresì tenuti a istituire uno o più CSIRT che siano incaricati di gestire gli incidenti, secondo un processo ben definito, e che si occupino almeno dei settori, dei sottosettori e dei tipi di soggetti

([15]) Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti (GU L 331 del 14.12.2017, p. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

([16]) 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).

([17]) 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).

che rientrano nell'ambito di applicazione di tale direttiva, nonché a garantire che i CSIRT dispongano di risorse adeguate per svolgere efficacemente i rispettivi compiti. Il presente regolamento non pregiudica il ruolo della Commissione di garantire il rispetto da parte degli Stati membri degli obblighi previsti dalla direttiva (UE) 2022/2555. Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire assistenza per azioni volte a rafforzare la preparazione e azioni di risposta agli incidenti intese ad attenuare l'impatto di incidenti di cibersicurezza significativi e di incidenti di cibersicurezza su vasta scala, al fine di sostenere la ripresa iniziale o il ripristino delle funzionalità essenziali dei servizi forniti dai soggetti che operano in settori ad alta criticità o ai soggetti che operano in altri settori critici.

(34) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori ad alta criticità individuati a norma della direttiva (UE) 2022/2555, anche tramite le esercitazioni e la formazione. A tal fine la Commissione, previa consultazione dell'ENISA, del gruppo di cooperazione NIS e di EU-CyCLONe, dovrebbe individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata di preparazione a livello dell'Unione. I settori o i sottosettori dovrebbero essere selezionati tra i settori ad alta criticità elencati all'allegato I della direttiva (UE) 2022/2555. La verifica coordinata di preparazione dovrebbe basarsi su scenari di rischio e metodologie comuni. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui si occupano la Commissione, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza («alto rappresentante») e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche istituito dal regolamento (UE) 2018/1971 del Parlamento europeo e del Consiglio ([18]), le valutazioni coordinate a livello dell'Unione del rischio di sicurezza delle catene di approvvigionamento critiche da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio ([19]). La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

(35) Il meccanismo per le emergenze di cibersicurezza dovrebbe inoltre fornire sostegno ad altre azioni di preparazione e sostenere la preparazione in altri settori non interessati dalla verifica coordinata di preparazione dei soggetti che operano in settori ad alta criticità o di soggetti che operano in altri settori critici. Tali azioni potrebbero includere vari tipi di attività di preparazione nazionali.

(36) Quando gli Stati membri ricevono sovvenzioni a sostegno di azioni di preparazione, i soggetti in settori ad alta criticità possono partecipare a tali azioni su base volontaria. È buona prassi che, a seguito di tali azioni, i soggetti partecipanti elaborino un piano di ripristino per attuare le raccomandazioni risultanti da misure specifiche al fine di trarre il massimo beneficio dall'azione di preparazione. Sebbene sia importante che gli Stati membri richiedano, nell'ambito delle azioni, che i soggetti partecipanti elaborino e attuino tali piani di ripristino, gli Stati membri non sono tenuti né autorizzati a dare esecuzione a tali richieste in virtù del presente regolamento. Tali richieste lasciano impregiudicati gli obblighi dei soggetti e i poteri di vigilanza delle autorità competenti di cui alla direttiva (UE) 2022/2555.

(37) Il meccanismo per le emergenze di cibersicurezza dovrebbe inoltre sostenere azioni di risposta agli incidenti volte ad attenuare l'impatto di incidenti di cibersicurezza significativi, di incidenti di cibersicurezza su vasta scala e di incidenti di cibersicurezza equivalenti a incidenti su vasta scala, al fine di favorire la ripresa iniziale o ripristinare il funzionamento di servizi essenziali. Ove opportuno, dovrebbe integrare l'UCPM per garantire un approccio globale di risposta all'impatto esercitato dagli incidenti sui cittadini.

([18]) Regolamento (UE) 2018/1971 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Agenzia di sostegno al BEREC (Ufficio BEREC), modifica il regolamento (UE) 2015/2120 e abroga il regolamento (CE) n. 1211/2009 (GU L 321 del 17.12.2018, pag. 1).

([19]) 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)

(38) Il meccanismo per le emergenze di cibersicurezza dovrebbe sostenere l'assistenza tecnica fornita da uno Stato membro a un altro Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o un incidente di cibersicurezza su vasta scala, anche mediante la rete di CSIRT di cui all'articolo 11, paragrafo 3, lettera f), della direttiva (UE) 2022/2555. Gli Stati membri che forniscono tale assistenza dovrebbero essere autorizzati a presentare richieste di copertura dei costi relativi all'invio di squadre di esperti nel quadro dell'assistenza reciproca. I costi ammissibili potrebbero includere le spese di viaggio e di alloggio nonché l'indennità giornaliera degli esperti di cibersicurezza.

(39) Dato il ruolo essenziale svolto dalle imprese private nel rilevamento degli incidenti di cibersicurezza su vasta scala e degli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e nella preparazione e risposta agli stessi, è importante riconoscere il valore della cooperazione volontaria a titolo gratuito con tali imprese, che offrono, in tale contesto, servizi senza remunerazione in caso di crisi e incidenti di cibersicurezza su vasta scala e di crisi e incidenti di cibersicurezza equivalenti a incidenti su vasta scala. L'ENISA, in cooperazione con EU-CyCLONe, potrebbe monitorare l'evoluzione di tali iniziative a titolo gratuito e promuoverne la conformità ai criteri applicabili ai fornitori di fiducia di servizi di sicurezza gestiti a norma del presente regolamento, anche per quanto riguarda l'affidabilità delle imprese private, la loro esperienza e la capacità di gestire informazioni sensibili in modo sicuro.

(40) Nell'ambito del meccanismo per le emergenze di cibersicurezza, è opportuno istituire gradualmente una riserva dell'UE per la cibersicurezza, costituita da servizi erogati da fornitori di fiducia di servizi di sicurezza gestiti per sostenere la risposta e avviare azioni di ripresa in caso di incidenti di cibersicurezza significativi, di incidenti di cibersicurezza su vasta scala e di incidenti di cibersicurezza equivalenti a incidenti su vasta scala che interessano gli Stati membri, le istituzioni, gli organi o organismi dell'Unione o i paesi terzi associati al programma Europa digitale. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi. Essa dovrebbe pertanto includere servizi che sono impegnati in anticipo, tra cui, ad esempio, capacità reperibili e mobilitabili con breve preavviso. I servizi della riserva dell'UE per la cibersicurezza dovrebbero servire a sostenere le autorità nazionali nel fornire assistenza ai soggetti colpiti che operano in settori ad alta criticità o ai soggetti colpiti che operano in altri settori critici, a integrazione delle azioni da esse svolte a livello nazionale. I servizi di tale riserva dovrebbero poter servire a sostenere le istituzioni, gli organi e gli organismi dell'Unione, in condizioni analoghe. La riserva dell'UE per la cibersicurezza potrebbe inoltre contribuire al rafforzamento della posizione competitiva del settore industriale e di quello dei servizi nell'Unione nell'ambito dell'economia digitale, tra l'altro per le microimprese e le piccole e medie imprese nonché le start-up, anche offrendo incentivi agli investimenti nell'ambito della ricerca e dell'innovazione. È importante tenere conto del quadro europeo in materia di competenze nel settore della cibersicurezza dell'ENISA in sede di acquisizione dei servizi per la riserva dell'UE per la cibersicurezza. Nel richiedere il sostegno della riserva dell'UE per la cibersicurezza, gli utenti dovrebbero includere nella loro domanda informazioni adeguate riguardanti il soggetto interessato e il potenziale impatto, informazioni sul servizio richiesto a carico della riserva dell'UE per la cybersicurezza e sul sostegno fornito al soggetto interessato a livello nazionale, che è opportuno prendere in considerazione nella valutazione della richiesta del richiedente. Al fine di garantire la complementarietà con altre forme di sostegno disponibili per il soggetto interessato, la richiesta dovrebbe altresì includere, ove disponibili, informazioni sugli accordi contrattuali in essere per servizi di risposta agli incidenti e di ripresa iniziale, nonché i contratti assicurativi potenzialmente in grado di coprire il tipo di incidente in questione.

(41) Al fine di garantire un uso efficace dei finanziamenti dell'Unione, i servizi preimpegnati nell'ambito della riserva dell'UE per la cibersicurezza dovrebbero essere convertibili, conformemente al pertinente contratto, in servizi di preparazione relativi alla prevenzione degli incidenti e alla risposta agli stessi nel caso in cui tali servizi preimpegnati non siano utilizzati per la risposta agli incidenti durante il periodo per il quale sono preimpegnati. Tali servizi dovrebbero essere complementari alle azioni di preparazione che saranno gestite dall'ECCC e non dovrebbero duplicarle.

(42) Le richieste di sostegno della riserva dell'UE per la cibersicurezza provenienti dalle autorità di gestione delle crisi informatiche e dai CSIRT degli Stati membri o dal CERT-UE per conto delle istituzioni, degli organi e degli organismi dell'Unione dovrebbero essere valutate dall'amministrazione aggiudicatrice. Se l'ENISA è stata incaricata dell'amministrazione e del funzionamento della riserva dell'UE per la cibersicurezza, tale amministrazione aggiudicatrice è l'ENISA stessa. Le richieste di sostegno da parte di paesi terzi associati al programma Europa digitale dovrebbero essere valutate dalla Commissione. Per facilitare la presentazione e la valutazione delle richieste di sostegno, l'ENISA potrebbe istituire una piattaforma sicura.

(43) Qualora siano ricevute più richieste concomitanti, dovrebbero essere attribuite delle priorità in base a criteri stabiliti nel presente regolamento. Alla luce degli obiettivi generali del presente regolamento, tali criteri dovrebbero includere la portata e la gravità dell'incidente, il tipo di soggetto interessato, il potenziale impatto dell'incidente sugli Stati membri e sugli utenti interessati, la potenziale natura transfrontaliera dell'incidente e il rischio di ricaduta e le misure già adottate dall'utente per assistere la risposta e la ripresa iniziale. Alla luce di tali obiettivi e dato che le richieste

degli utenti degli Stati membri sono intese esclusivamente a sostenere, in tutta l'Unione, soggetti che operano in settori ad alta criticità o soggetti che operano in altri settori critici, è opportuno attribuire maggiore priorità alle richieste degli utenti degli Stati membri qualora due o più richieste siano considerate di pari valore in base a tali criteri. Ciò lascia impregiudicati gli obblighi che gli Stati membri possono avere, in virtù delle pertinenti convenzioni di accoglienza, di adottare misure per proteggere e assistere le istituzioni, gli organi e gli organismi dell'Unione.

(44) La Commissione dovrebbe avere la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza. Data l'ampia esperienza acquisita dall'ENISA con l'azione di sostegno alla cibersicurezza, l'ENISA è l'agenzia più adatta per attuare la riserva dell'UE per la cibersicurezza. Pertanto, la Commissione dovrebbe affidare all'ENISA in parte o, se la Commissione lo ritiene opportuno, interamente il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza. L'incarico dovrebbe essere affidato conformemente alle norme applicabili a norma del regolamento (UE, Euratom) 2024/2509 e, in particolare, dovrebbe essere subordinato al rispetto delle condizioni pertinenti per la firma di un accordo di contributo. Tutti gli aspetti relativi al funzionamento e all'amministrazione della riserva dell'UE per la cibersicurezza non affidati all'ENISA dovrebbero essere soggetti alla gestione diretta da parte della Commissione, anche prima della firma dell'accordo di contributo.

(45) Gli Stati membri dovrebbero svolgere un ruolo chiave nella costituzione, nella mobilitazione e nella fase successiva alla mobilitazione della riserva dell'UE per la cibersicurezza. Poiché il regolamento (UE) 2021/694 è il pertinente atto di base per le azioni di attuazione della riserva dell'UE per la cibersicurezza, le azioni nell'ambito della riserva dell'UE per la cibersicurezza dovrebbero essere previste nei programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694. A norma del paragrafo 6 di tale articolo, i programmi di lavoro devono essere adottati dalla Commissione mediante atti di esecuzione secondo la procedura d'esame. Inoltre, la Commissione, in coordinamento con il gruppo di cooperazione NIS, dovrebbe determinare le priorità e l'evoluzione della riserva dell'UE per la cibersicurezza.

(46) I contratti conclusi nel quadro della riserva dell'UE per la cibersicurezza non dovrebbero incidere sul rapporto tra imprese e sugli obblighi esistenti tra il soggetto interessato o gli utenti, da un lato, e il fornitore di servizi, dall'altro.

(47) Ai fini della selezione di fornitori di servizi privati per la prestazione di servizi nel contesto della riserva dell'UE per la cibersicurezza, occorre stabilire una serie di criteri e requisiti minimi da includere nel corrispondente bando di gara, in modo da garantire che siano soddisfatte le esigenze delle autorità degli Stati membri, dei soggetti che operano in settori ad alta criticità e dei soggetti che operano in altri settori critici. Al fine di rispondere alle esigenze specifiche degli Stati membri, in sede di acquisizione di servizi per la riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice dovrebbe, se del caso, elaborare criteri di selezione e requisiti aggiuntivi rispetto a quelli stabiliti nel presente regolamento. È importante incoraggiare la partecipazione dei fornitori più piccoli, attivi a livello regionale e locale.

(48) Nel selezionare i fornitori da includere nella riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice dovrebbe mirare a garantire che la riserva dell'UE per la cibersicurezza, se considerata nel suo insieme, contenga fornitori in grado di soddisfare i requisiti linguistici degli utenti. A tal fine, prima di preparare il capitolato d'oneri l'amministrazione aggiudicatrice dovrebbe verificare se i potenziali utenti della riserva dell'UE per la cibersicurezza abbiano requisiti linguistici specifici, in modo che i servizi di sostegno della riserva dell'UE per la cibersicurezza possano essere forniti in una lingua tra le lingue ufficiali delle istituzioni dell'Unione o degli Stati membri che possa essere compresa dall'utente o dal soggetto interessato. Qualora un utente richieda più di una lingua per la fornitura di servizi di supporto della riserva dell'UE per la cibersicurezza e tali servizi siano stati acquistati in tali lingue per tale utente, l'utente dovrebbe poter specificare, nella richiesta di sostegno della riserva dell'UE per la cibersicurezza, in quali di tali lingue dovrebbero essere forniti i servizi in relazione all'incidente specifico che ha dato origine alla richiesta.

(49) Al fine di sostenere l'istituzione della riserva dell'UE per la cibersicurezza, è importante che la Commissione chieda all'ENISA di preparare una proposta di sistema di certificazione in materia di cibersicurezza per i servizi di sicurezza gestiti ai sensi del regolamento (UE) 2019/881 nei settori che rientrano nel meccanismo per le emergenze di cibersicurezza.

(50) Al fine di sostenere gli obiettivi del presente regolamento di promuovere la condivisione della conoscenza situazionale, rafforzare la resilienza dell'Unione e consentire una risposta efficace agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, la Commissione o EU-CyCLONe dovrebbero poter richiedere all'ENISA, con il supporto della rete di CSIRT e con il consenso dello Stato membro interessato, di riesaminare e valutare le minacce informatiche, le vulnerabilità sfruttabili note e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o incidente di cibersicurezza su vasta scala. A seguito del completamento del riesame e della valutazione di un incidente, l'ENISA dovrebbe preparare una

relazione di riesame dell'incidente, in collaborazione con lo Stato membro interessato, i pertinenti portatori di interessi, compresi i rappresentanti del settore privato, la Commissione e altre istituzioni, organi e organismi dell'Unione pertinenti. Basandosi sulla collaborazione con i portatori di interessi, compreso il settore privato, la relazione di riesame riguardante incidenti specifici dovrebbe mirare a valutare le cause, l'impatto e le misure di attenuazione di un incidente una volta verificatosi. È opportuno prestare particolare attenzione ai contributi e agli insegnamenti condivisi dai fornitori di servizi di sicurezza gestiti che soddisfano le condizioni di massima integrità professionale, imparzialità e competenza tecnica necessaria imposte dal presente regolamento. La relazione dovrebbe essere presentata a EU-CyCLONe, alla rete di CSIRT e alla Commissione e dovrebbe essere utilizzata per informare le loro attività e quelle dell'ENISA. Se l'incidente riguarda un paese terzo associato al programma Europa digitale, la Commissione dovrebbe fornire la relazione anche all'alto rappresentante.

(51) Tenendo conto della natura imprevedibile degli attacchi informatici e del fatto che spesso non sono circoscritti a un'area geografica specifica e presentano un elevato rischio di propagazione, il rafforzamento della resilienza dei paesi limitrofi e della loro capacità di rispondere efficacemente agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala contribuisce alla protezione dell'Unione nel suo complesso, in particolare del suo mercato interno e della sua industria. Tali attività potrebbero contribuire ulteriormente alla diplomazia informatica dell'Unione. I paesi terzi associati al programma Europa digitale dovrebbero quindi poter richiedere supporto alla riserva dell'UE per la cibersicurezza, in tutti i loro territori o in parte di essi, laddove ciò sia previsto dall'accordo attraverso il quale il paese terzo è associato al programma Europa digitale. Il finanziamento per i paesi terzi associati al programma Europa digitale dovrebbe essere sostenuto dall'Unione nel quadro dei partenariati e degli strumenti di finanziamento pertinenti per tali paesi. Il sostegno dovrebbe riguardare servizi nell'ambito della risposta e della ripresa iniziale in caso di incidenti di cibersicurezza significativi o incidenti di cibersicurezza equivalenti a incidenti su vasta scala.

(52) Le condizioni stabilite per la riserva dell'UE per la cibersicurezza e per i fornitori di fiducia di servizi di sicurezza gestiti nel presente regolamento dovrebbero essere applicate quando è fornito sostegno ai paesi terzi associati al programma Europa digitale. I paesi terzi associati al programma Europa digitale dovrebbero poter richiedere sostegno alla riserva dell'UE per la cibersicurezza quando i soggetti interessati e per i quali chiedono il sostegno della riserva dell'UE per la cibersicurezza sono soggetti che operano in settori ad alta criticità o soggetti che operano in altri settori critici e quando gli incidenti individuati comportano perturbazioni operative significative o potrebbero avere effetti di ricaduta nell'Unione. I paesi terzi associati al programma Europa digitale dovrebbero essere ammissibili al sostegno solo se l'accordo attraverso il quale sono associati al programma Europa digitale prevede specificamente tale sostegno. Inoltre, tali paesi terzi dovrebbero rimanere ammissibili solo a condizione che siano soddisfatti tre criteri. In primo luogo, il paese terzo dovrebbe rispettare pienamente i termini pertinenti di tale accordo. In secondo luogo, data la natura complementare della riserva dell'UE per la cibersicurezza, il paese terzo avrebbe dovuto adottare misure adeguate per prepararsi a incidenti di cibersicurezza significativi o a incidenti di cibersicurezza equivalenti a incidenti su vasta scala. In terzo luogo, il sostegno fornito dalla riserva dell'UE per la cibersicurezza dovrebbe essere coerente con la politica dell'Unione nei confronti del paese e con le sue relazioni generali con il paese nonché con altre politiche dell'Unione in materia di sicurezza. Nel contesto della valutazione della conformità a tale terzo criterio, la Commissione dovrebbe consultare l'alto rappresentante per allineare la concessione di tale sostegno alla politica estera e di sicurezza comune.

(53) La fornitura di sostegno ai paesi terzi associati al programma Europa digitale può incidere sulle relazioni con i paesi terzi e sulla politica di sicurezza dell'Unione, anche nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune. È pertanto opportuno che al Consiglio siano attribuite competenze di esecuzione per autorizzare e specificare il periodo durante il quale tale sostegno può essere fornito. Il Consiglio dovrebbe deliberare sulla base di una proposta della Commissione, tenendo debitamente conto della valutazione da parte della Commissione dei tre criteri. Lo stesso dovrebbe valere per i rinnovi e per le proposte di modifica o abrogazione di tali atti. Qualora, in circostanze eccezionali, ritenga che vi sia stato un cambiamento significativo delle circostanze in relazione al terzo criterio, il Consiglio dovrebbe poter agire di propria iniziativa per modificare o abrogare un atto di esecuzione, senza attendere una proposta della Commissione. Tali cambiamenti significativi richiederanno probabilmente un'azione urgente, avranno implicazioni particolarmente importanti per le relazioni con i paesi terzi e non richiederanno una valutazione approfondita in anticipo da parte della Commissione. Inoltre, la Commissione dovrebbe cooperare con l'alto rappresentante in relazione alle richieste di sostegno da parte dei paesi terzi associati al programma Europa digitale e all'attuazione di tale sostegno. La Commissione dovrebbe tenere anche conto di eventuali pareri forniti dall'ENISA in merito alle medesime richieste e al medesimo sostegno. La Commissione dovrebbe informare il Consiglio in merito all'esito della valutazione delle richieste, comprese le pertinenti considerazioni formulate al riguardo, e ai servizi mobilitati.

(54) La comunicazione della Commissione del 18 aprile 2023 sull'Accademia per le competenze in materia di cibersicurezza ha riconosciuto la carenza di professionisti qualificati. Tali competenze sono necessarie per perseguire gli obiettivi del presente regolamento. L'Unione ha urgentemente bisogno di professionisti dotati di capacità e competenze per prevenire, individuare e scoraggiare gli attacchi informatici e difendere l'Unione, comprese le sue infrastrutture più critiche, da tali attacchi e garantirne la resilienza. A tal fine, è importante incoraggiare la cooperazione tra le parti interessate, comprese quelle appartenenti al settore privato, al mondo accademico e al settore pubblico. È altrettanto importante creare sinergie, in tutti i territori dell'Unione, per gli investimenti nell'istruzione e nella formazione, al fine di promuovere la creazione di misure di salvaguardia per evitare la fuga di cervelli o un allargamento del divario di competenze in alcune regioni più che in altre. È urgente colmare il divario di competenze in materia di cibersicurezza, con particolare attenzione alla riduzione del divario di genere nella forza lavoro nel settore della cibersicurezza, al fine di promuovere la presenza e la partecipazione delle donne alla progettazione della governance digitale.

(55) Al fine di stimolare l'innovazione nel mercato unico digitale, è importante rafforzare la ricerca e l'innovazione nel settore della cibersicurezza, allo scopo di contribuire ad aumentare la resilienza degli Stati membri e l'autonomia strategica aperta dell'Unione, entrambi obiettivi del presente regolamento. Le sinergie sono essenziali per rafforzare la cooperazione e il coordinamento tra le diverse parti interessate, tra cui quelle appartenenti al settore privato, alla società civile e al mondo accademico.

(56) Il presente regolamento dovrebbe tener conto dell'impegno enunciato nella dichiarazione comune del 26 gennaio 2022 del Parlamento europeo, del Consiglio e della Commissione dal titolo «Dichiarazione europea sui diritti e i principi digitali per il decennio digitale» per proteggere gli interessi delle democrazie, dei cittadini, delle imprese e delle istituzioni pubbliche dell'Unione dai rischi di cibersicurezza e dalla criminalità informatica, comprese le violazioni dei dati e il furto o la manipolazione dell'identità.

(57) Al fine di integrare alcuni elementi non essenziali del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE al fine di specificare le tipologie e il numero dei servizi di risposta richiesti per la riserva dell'UE per la 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 ([20]). 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.

(58) Al fine di garantire condizioni uniformi di attuazione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione per specificare ulteriormente le modalità procedurali dettagliate per l'assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([21]).

(59) Fatte salve le norme relative al bilancio annuale dell'Unione a norma dei trattati, la Commissione dovrebbe tenere conto degli obblighi derivanti dal presente regolamento nel valutare il fabbisogno di bilancio e di personale dell'ENISA.

(60) La Commissione dovrebbe effettuare periodicamente una valutazione delle misure di cui al presente regolamento. La prima di tali valutazioni dovrebbe aver luogo nei primi due anni dopo la data di entrata in vigore del presente regolamento e successivamente almeno ogni quattro anni, tenendo conto del calendario della revisione del quadro finanziario pluriennale istituito a norma dell'articolo 312 TFUE. La Commissione dovrebbe presentare al Parlamento europeo e al Consiglio una relazione sui progressi realizzati. Al fine di valutare i diversi elementi richiesti, compresa la portata delle informazioni condivise nell'ambito del sistema europeo di allerta per la cibersicurezza, la Commissione dovrebbe basarsi esclusivamente su informazioni prontamente disponibili o fornite volontariamente. Tenendo in considerazione gli sviluppi geopolitici e al fine di garantire la continuità e l'ulteriore sviluppo delle misure stabilite nel presente regolamento dopo il 2027, è importante che la Commissione valuti la necessità di assegnare un bilancio appropriato al quadro finanziario pluriennale per il periodo 2028-2034.

([20]) GU L 123 del 12.5.2016, pag. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([21]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Poiché gli obiettivi del presente regolamento, vale a dire rafforzare la posizione competitiva dell'industria e dei servizi nell'Unione in tutta l'economia digitale e contribuire alla sovranità tecnologica e all'autonomia strategica aperta dell'Unione nel settore della cibersicurezza, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della portata e gli 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. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, in particolare mediante l'istituzione di:

a) una rete paneuropea di poli informatici (il sistema europeo di allerta per la cibersicurezza) per sviluppare e potenziare capacità coordinate in materia di rilevamento e capacità comuni in materia di conoscenza situazionale;

b) un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, nella mitigazione del loro impatto e nella ripresa dagli stessi, e per sostenere gli altri utenti nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala;

c) un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di incidenti di cibersicurezza significativi o incidenti di cibersicurezza su vasta scala.

2. Il presente regolamento persegue gli obiettivi generali di rafforzare la posizione competitiva del settore industriale e di quello dei servizi nell'Unione nell'ambito dell'economia digitale, tra l'altro per le microimprese e le piccole e medie imprese nonché le start-up, e di contribuire alla sovranità tecnologica dell'Unione e all'autonomia strategica aperta nel campo della cibersicurezza, anche potenziando l'innovazione del mercato unico digitale. Persegue tali obiettivi rafforzando la solidarietà a livello dell'Unione, potenziando l'ecosistema della cibersicurezza, migliorando la resilienza informatica degli Stati membri e sviluppando le competenze, il know-how, le capacità e le competenze della forza lavoro in relazione alla cibersicurezza.

3. Il conseguimento degli obiettivi generali di cui al paragrafo 2 è perseguito mediante gli obiettivi specifici seguenti:

a) migliorare le capacità coordinate di rilevamento e le capacità di conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici;

b) rafforzare la preparazione dei soggetti che operano in settori ad alta criticità o dei soggetti che operano in altri settori critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di verifica coordinata della preparazione, di risposta potenziata e di ripresa per gestire incidenti di cibersicurezza significativi, incidenti di cibersicurezza su vasta scala o incidenti di cibersicurezza equivalenti a incidenti su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;

c) accrescere la resilienza dell'Unione e contribuire a una risposta efficace agli incidenti, riesaminando e valutando gli incidenti di cibersicurezza significativi o gli incidenti di cibersicurezza su vasta scala, traendone anche insegnamenti e, se del caso, formulando raccomandazioni.

4. Le azioni intraprese a norma del presente regolamento sono realizzate nel debito rispetto delle competenze degli Stati membri e integrano le attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS.

5. Il presente regolamento lascia impregiudicate le funzioni statali essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale dello Stato, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale. In particolare, la sicurezza nazionale resta una competenza esclusiva di ciascuno Stato membro.

6. La condivisione o lo scambio di informazioni ai sensi del presente regolamento che sono riservate ai sensi della normativa dell'Unione o nazionale sono limitati a quanto pertinente e proporzionato allo scopo di tale condivisione o scambio. L condivisione o lo scambio di informazioni devono tutelare la riservatezza delle informazioni e proteggere la sicurezza e gli interessi commerciali dei soggetti interessati. Ciò non deve comportare la comunicazione di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «polo informatico transfrontaliero»: una piattaforma multinazionale, istituita mediante un accordo di consorzio scritto, che riunisce in una struttura di rete coordinata i poli informatici nazionali di almeno tre Stati membri e che è concepita per migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche, per impedire gli incidenti informatici e per favorire l'elaborazione di analisi delle minacce informatiche, in particolare mediante lo scambio di dati e informazioni pertinenti, se del caso anonimizzati, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;

2) «consorzio ospitante»: un consorzio composto da Stati membri partecipanti che hanno concordato di stabilire e sostenere l'acquisizione di strumenti, infrastrutture o servizi per un polo informatico transfrontaliero e il suo funzionamento;

3) «CSIRT»: un CSIRT designato o istituito a norma dell'articolo 10 della direttiva (UE) 2022/2555;

4) «soggetto»: un soggetto quale definito all'articolo 6, punto 38), della direttiva (UE) 2022/2555;

5) «soggetti che operano in settori ad alta criticità»: i tipi di soggetti elencati nell'allegato I della direttiva (UE) 2022/2555;

6) «soggetti che operano in altri settori critici»: i tipi di soggetti elencati nell'allegato II alla direttiva (UE) 2022/2555;

7) «rischio»: un rischio quale definito all'articolo 6, punto 9), della direttiva (UE) 2022/2555;

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

9) «incidente»: un incidente quale definito all'articolo 6, punto 6), della direttiva (UE) 2022/2555;

(10) «incidente di cibersicurezza significativo»: un incidente che soddisfa i criteri stabiliti all'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555;

11) «incidente grave»: un incidente grave quale definito all'articolo 3, punto 8), del regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio ([22]);

12) «incidente di cibersicurezza su vasta scala»: un incidente di cibersicurezza su vasta scala quale definito all'articolo 6, punto 7), della direttiva (UE) 2022/2555;

([22]) Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) «incidente di cibersicurezza equivalente a incidenti su vasta scala»: nel caso delle istituzioni, degli organi e degli organismi dell'Unione, un incidente grave e, nel caso di paesi terzi associati al programma Europa digitale, un incidente che causa un livello di perturbazione superiore alla capacità di un paese terzo associato al programma Europa digitale di rispondervi;

14) «paese terzo associato al programma Europa digitale»: un paese terzo che è parte di un accordo con l'Unione che ne consente la partecipazione al programma Europa digitale a norma dell'articolo 10 del regolamento (UE) 2021/694;

15) «amministrazione aggiudicatrice»: la Commissione o, nella misura in cui il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza sono stati affidati all'ENISA a norma dell'articolo 14, paragrafo 5, del presente regolamento, l'ENISA;

16) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi di sicurezza gestiti quale definito all'articolo 6, punto 40), della direttiva (UE) 2022/2555;

17) «fornitori di fiducia di servizi di sicurezza gestiti»: fornitori di servizi di sicurezza gestiti selezionati per essere inclusi nella riserva dell'UE per la cibersicurezza in conformità dell'articolo 17.

CAPO II

IL SISTEMA EUROPEO DI ALLERTA PER LA CIBERSICUREZZA

Articolo 3

Istituzione del sistema europeo di allerta per la cibersicurezza

1. È istituito il sistema europeo di allerta per la cibersicurezza, una rete paneuropea di infrastrutture costituita da poli informatici nazionali e poli informatici transfrontalieri che aderiscono su base volontaria, per sostenere lo sviluppo di capacità avanzate affinché l'Unione migliori le capacità di rilevamento, analisi e trattamento dei dati in relazione alle minacce informatiche e la prevenzione degli incidenti nell'Unione.

2. Il sistema europeo di allerta per la cibersicurezza ha le funzioni seguenti:

a) contribuire a una migliore protezione dalle minacce informatiche e a migliori risposte alle stesse sostenendo i soggetti pertinenti, in particolare i CSIRT, la rete di CSIRT, EU-CyCLONe e le autorità competenti designate o istituite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, cooperando con essi e rafforzandone le capacità;

b) mettere in comune i dati e le informazioni pertinenti sulle minacce e sugli incidenti informatici provenienti da varie fonti all'interno dei poli informatici transfrontalieri e condividere informazioni analizzate o aggregate attraverso i poli informatici transfrontalieri, se del caso con la rete di CSIRT;

c) raccogliere e sostenere la produzione di analisi sulle minacce informatiche e informazioni di alta qualità e fruibili mediante l'uso di strumenti all'avanguardia e di tecnologie avanzate, e condividere tali analisi sulle minacce informatiche e informazioni;

d) contribuire a migliorare il rilevamento coordinato delle minacce informatiche e la conoscenza situazionale comune in tutta l'Unione, nonché all'emissione di segnalazioni, anche, se del caso, fornendo raccomandazioni concrete ai soggetti;

e) fornire servizi e attività per la comunità di cibersicurezza nell'Unione, compreso il contributo allo sviluppo di strumenti e tecnologie avanzati, come gli strumenti di intelligenza artificiale e di analisi dei dati.

3. Le azioni di attuazione del sistema europeo di allerta per la cibersicurezza sono sostenute da finanziamenti del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694, in particolare dell'obiettivo specifico 3.

Articolo 4

Poli informatici nazionali

1. Qualora decida di partecipare al sistema europeo di allerta per la cibersicurezza, uno Stato membro designa o, se del caso, istituisce un polo informatico nazionale ai fini del presente regolamento.

2. Il polo informatico nazionale è un soggetto unico che agisce sotto l'autorità di uno Stato membro. Può trattarsi di un CSIRT o, se del caso, di un'autorità nazionale di gestione delle crisi informatiche o di un'altra autorità competente designata o istituita a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, o di un altro soggetto. Il polo informatico nazionale:

a) ha la capacità di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti informatici e per contribuire a un polo informatico transfrontaliero di cui all'articolo 5; e

b) è in grado di rilevare, aggregare e analizzare dati e informazioni relativi alle minacce e agli incidenti informatici, come le analisi sulle minacce informatiche, utilizzando in particolare tecnologie all'avanguardia, al fine di prevenire gli incidenti.

3. Nell'ambito delle funzioni di cui al paragrafo 2 del presente articolo, i poli informatici nazionali possono cooperare con soggetti del settore privato per scambiare dati e informazioni pertinenti al fine di individuare e prevenire minacce e incidenti informatici, anche con le comunità settoriali e intersettoriali di soggetti essenziali e importanti di cui all'articolo 3 della direttiva (UE) 2022/2555. Se del caso e conformemente al diritto dell'Unione e nazionale, le informazioni richieste o ricevute dai poli informatici nazionali possono includere dati raccolti mediante telemetria, sensori e registrazioni.

4. Uno Stato membro selezionato a norma dell'articolo 9, paragrafo 1, si impegna a chiedere che il proprio polo informatico nazionale partecipi a un polo informatico transfrontaliero.

Articolo 5

Poli informatici transfrontalieri

1. Qualora almeno tre Stati membri siano impegnati a garantire che i rispettivi poli informatici nazionali collaborino per coordinare le loro attività di rilevamento e di monitoraggio delle minacce informatiche, tali Stati membri possono istituire un consorzio ospitante ai fini del presente regolamento.

2. Un consorzio ospitante è composto da almeno tre Stati membri partecipanti che abbiano concordato di stabilire e sostenere l'acquisizione di strumenti, infrastrutture o servizi per un polo informatico transfrontaliero conformemente al paragrafo 4, e per il suo funzionamento.

3. Se un consorzio ospitante è selezionato a norma dell'articolo 9, paragrafo 3, i suoi membri stipulano un accordo di consorzio scritto che:

a) definisce le disposizioni interne per l'attuazione della convezione di accoglienza e di utilizzo di cui all'articolo 9, paragrafo 3;

b) istituisce il polo informatico transfrontaliero del consorzio ospitante; e

c) include le clausole specifiche richieste a norma dell'articolo 6, paragrafi 1 e 2.

4. Un polo informatico transfrontaliero è una piattaforma multinazionale istituita da un accordo di consorzio scritto di cui al paragrafo 3. Riunisce in una struttura di rete coordinata i poli informatici nazionali degli Stati membri del consorzio ospitante. È concepito per migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche, per impedire gli incidenti e per favorire l'elaborazione di analisi delle minacce informatiche, in particolare mediante lo scambio di dati e informazioni pertinenti, se del caso anonimizzati, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia.

5. Un polo informatico transfrontaliero è rappresentato a fini legali da un membro del consorzio ospitante corrispondente che funge da coordinatore o dal consorzio ospitante se quest'ultimo ha personalità giuridica. La responsabilità della conformità da parte del polo informatico transfrontaliero al presente regolamento e alla convenzione di accoglienza e di utilizzo è assegnata nell'accordo di consorzio scritto di cui al paragrafo 3.

6. Uno Stato membro può aderire a un consorzio ospitante esistente mediante l'accordo dei membri del consorzio ospitante. L'accordo di consorzio scritto di cui al paragrafo 3 e la convenzione di accoglienza e di utilizzo sono modificati di conseguenza. Ciò non pregiudica i diritti di proprietà del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC) sugli strumenti, le infrastrutture o i servizi già acquisiti congiuntamente con tale consorzio ospitante.

Articolo 6

Cooperazione e condivisione di informazioni tra poli informatici transfrontalieri e al loro interno

1. I membri di un consorzio ospitante assicurano che i loro poli informatici nazionali condividano tra loro, conformemente all'accordo di consorzio scritto di cui all'articolo 5, paragrafo 3, informazioni pertinenti, se del caso anonimizzati, quali informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cibersicurezza e raccomandazioni relative alla configurazione degli strumenti di cibersicurezza per rilevare gli attacchi informatici, tra loro all'interno del polo informatico transfrontaliero, laddove tale condivisione di informazioni:

a) promuova e migliori il rilevamento delle minacce informatiche e rafforzi le capacità della rete di CSIRT di prevenire e rispondere agli incidenti o di attenuarne l'impatto;

b) accresca il livello di cibersicurezza, ad esempio 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, fasi di risposta e ripresa, o promuovendo la ricerca collaborativa sulle minacce tra soggetti pubblici e privati.

2. L'accordo di consorzio scritto di cui all'articolo 5, paragrafo 3, stabilisce:

a) l'impegno a condividere tra i membri del consorzio ospitante le informazioni di cui al paragrafo 1 e le condizioni di condivisione di tali informazioni;

b) un quadro di governance che chiarisca e incentivi la condivisione da parte di tutti i partecipanti di informazioni pertinenti, se del caso anonimizzati, di cui al paragrafo 1;

c) obiettivi per contribuire allo sviluppo di strumenti e tecnologie avanzati, quali gli strumenti di intelligenza artificiale e di analisi dei dati.

L'accordo di consorzio scritto può specificare che le informazioni di cui al paragrafo 1 devono essere condivise in conformità del diritto dell'Unione e nazionale.

3. I poli informatici transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di interoperabilità e di condivisione delle informazioni tra i poli informatici transfrontalieri. I poli informatici transfrontalieri informano la Commissione in merito agli accordi di cooperazione conclusi.

4. La condivisione delle informazioni di cui al paragrafo 1 tra i poli informatici transfrontalieri è garantito da un elevato livello di interoperabilità. Al fine di sostenere tale interoperabilità, l'ENISA, in stretta consultazione con la Commissione, senza indebito ritardo e in ogni caso entro il 5 febbraio 2026, emana orientamenti sull'interoperabilità che specificano in particolare formati e protocolli per la condivisione delle informazioni, tenendo conto delle norme e delle migliori pratiche internazionali, nonché del funzionamento di eventuali poli informatici transfrontalieri esistenti. I requisiti di interoperabilità previsti dagli accordi di cooperazione dei poli informatici transfrontalieri si basano sugli orientamenti emanati dall'ENISA.

Articolo 7

Cooperazione e condivisione di informazioni con reti a livello dell'Unione

1. I poli informatici transfrontalieri e la rete di CSIRT cooperano strettamente, in particolare al fine di condividere le informazioni. A tal fine, concordano le modalità procedurali in materia di cooperazione e condivisione delle informazioni pertinenti e, fatto salvo il paragrafo 2, circa i tipi di informazioni da condividere.

2. Quando ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, i poli informatici transfrontalieri garantiscono, ai fini della conoscenza situazionale comune, che le informazioni pertinenti e gli allarmi rapidi siano forniti senza indebito ritardo alle autorità degli Stati membri e alla Commissione attraverso EU-CyCLONe e la rete di CSIRT.

Articolo 8

Sicurezza

1. Gli Stati membri che partecipano al sistema europeo di allerta per la cibersicurezza garantiscono un elevato livello di cibersicurezza, comprese la riservatezza e la sicurezza dei dati, nonché la sicurezza fisica della rete del sistema europeo di allerta per la cibersicurezza e assicurano che la rete sia adeguatamente gestita e controllata, in modo da proteggerla dalle minacce e da garantire la sua sicurezza e quella dei sistemi, compresa quella dei dati e delle informazioni condivisi attraverso la rete.

2. Gli Stati membri che partecipano al sistema europeo di allerta per la cibersicurezza garantiscono che la condivisione di informazioni di cui all'articolo 6, paragrafo 1, nell'ambito del sistema europeo di allerta per la cibersicurezza con soggetti diversi da un'autorità pubblica o da un organismo pubblico di uno Stato membro non influisca negativamente sugli interessi di sicurezza dell'Unione o degli Stati membri.

Articolo 9

Finanziamento del sistema europeo di allerta per la cibersicurezza

1. A seguito di un invito a manifestare interesse per gli Stati membri che intendano partecipare al sistema europeo di allerta per la cibersicurezza, l'ECCC seleziona degli Stati membri per partecipare insieme all'appalto congiunto di strumenti, infrastrutture o servizi al fine di istituire poli informatici nazionali designati o stabiliti a norma dell'articolo 4, paragrafo 1, o di rafforzarne le capacità. L'ECCC può attribuire sovvenzioni agli Stati membri selezionati per finanziare il funzionamento di tali strumenti, infrastrutture o servizi. Il contributo finanziario dell'Unione copre fino al 50 % dei costi di acquisizione di strumenti, infrastrutture o servizi e fino al 50 % dei costi operativi. Gli Stati membri selezionati coprono i costi restanti. Prima di avviare la procedura di acquisizione di strumenti, infrastrutture o servizi, l'ECCC e gli Stati membri selezionati concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti, delle infrastrutture o dei servizi.

2. Ove un polo informatico nazionale di uno Stato membro non partecipi a un polo informatico transfrontaliero entro due anni dalla data di acquisizione degli strumenti, delle infrastrutture o dei servizi o, se precedente, dalla data in cui ha ricevuto la sovvenzione, lo Stato membro non può beneficiare dell'ulteriore sostegno dell'Unione ai sensi del presente capo fino a quando non abbia aderito a un polo informatico transfrontaliero.

3. A seguito di un invito a manifestare interesse, un consorzio ospitante è selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti, infrastrutture o servizi. L'ECCC può attribuire al consorzio ospitante una sovvenzione per finanziare il funzionamento degli strumenti, delle infrastrutture o dei servizi. Il contributo finanziario dell'Unione copre fino al 75 % dei costi di acquisizione degli strumenti, delle infrastrutture o dei servizi e fino al 50 % dei costi operativi. Il consorzio ospitante copre i costi restanti. Prima di avviare la procedura di acquisizione di strumenti, infrastrutture o servizi, l'ECCC e il consorzio ospitante concludono una convenzione di accoglienza e di utilizzo che disciplina l'uso degli strumenti, delle infrastrutture o dei servizi.

4. L'ECCC prepara, almeno ogni due anni, una mappatura degli strumenti, delle infrastrutture o dei servizi necessari e di qualità adeguata per istituire i poli informatici nazionali e i poli informatici transfrontalieri o rafforzarne le capacità, e della loro disponibilità, anche presso i soggetti giuridici stabiliti o ritenuti stabiliti negli Stati membri e controllati dagli Stati membri o da cittadini degli Stati membri. Nel preparare la mappatura, l'ECCC consulta la rete di CSIRT, i poli informatici transfrontalieri esistenti, l'ENISA e la Commissione.

CAPO III

MECCANISMO PER LE EMERGENZE DI CIBERSICUREZZA

Articolo 10

Istituzione del meccanismo per le emergenze di cibersicurezza

1. È istituito un meccanismo per le emergenze di cibersicurezza al fine di sostenere il miglioramento della resilienza dell'Unione alle minacce informatiche e, in uno spirito di solidarietà, la preparazione all'impatto a breve termine degli incidenti di cibersicurezza significativi, degli incidenti di sicurezza su vasta scala e degli incidenti di cibersicurezza equivalenti a incidenti su vasta scala, nonché attenuare tale impatto.

2. Nel caso degli Stati membri, le azioni nell'ambito del meccanismo per le emergenze di cibersicurezza sono svolte su richiesta e sono complementari agli sforzi e alle azioni degli Stati membri volti a prepararsi e rispondere agli incidenti nonché a riprendersi dai medesimi.

3. Le azioni di attuazione del meccanismo per le emergenze di cibersicurezza sono sostenute da finanziamenti a titolo del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694, in particolare dell'obiettivo specifico 3.

4. Le azioni nell'ambito del meccanismo per le emergenze di cibersicurezza sono attuate principalmente mediante l'ECCC in conformità del regolamento (UE) 2021/887. Tuttavia, le azioni di attuazione della riserva dell'UE per la cibersicurezza di cui all'articolo 11, lettera b), del presente regolamento sono attuate dalla Commissione e dall'ENISA.

Articolo 11

Tipi di azione

Il meccanismo per le emergenze di cibersicurezza sostiene i tipi di azioni seguenti:

a) azioni di preparazione, in particolare:

   i) la verifica coordinata della preparazione dei soggetti che operano in settori ad alta criticità in tutta l'Unione, come specificato all'articolo 12;

   ii) altre azioni di preparazione per i soggetti che operano in settori altamente critici o i soggetti che operano in altri settori critici, come specificato all'articolo 13;

b) azioni a sostegno della risposta agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e che avviano la ripresa dagli stessi, che devono essere svolte da fornitori di fiducia di servizi di sicurezza gestiti che partecipano alla riserva dell'UE per la cibersicurezza istituita ai sensi dell'articolo 14;

c) azioni a sostegno dell'assistenza reciproca di cui all'articolo 18.

Articolo 12

Verifica coordinata della preparazione dei soggetti

1. Il meccanismo per le emergenze di cibersicurezza sostiene la verifica volontaria coordinata della preparazione dei soggetti che operano in settori ad alta criticità.

2. La verifica coordinata della preparazione può consistere in attività di preparazione, quali i test di penetrazione, e nella valutazione delle minacce.

3. Il sostegno alle azioni di preparazione di cui al presente articolo è fornito agli Stati membri principalmente sotto forma di sovvenzioni e alle condizioni disposte nei pertinenti programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694.

4. Al fine di sostenere la verifica coordinata della preparazione dei soggetti di cui all'articolo 11, lettera a), punto i), del presente regolamento in tutta l'Unione, previa consultazione con il gruppo di cooperazione NIS, EU-CyCLONe e l'ENISA la Commissione individua i settori o i sottosettori interessati, a partire dai settori ad alta criticità elencati all'allegato I della

direttiva (UE) 2022/2555, per i quali può essere pubblicato un invito a presentare proposte per la concessione di sovvenzioni. La partecipazione degli Stati membri a tali inviti a presentare proposte avviene su base volontaria.

5. Nell'individuare i settori o sottosettori di cui al paragrafo 4, la Commissione tiene conto delle valutazioni coordinate del rischio e dei test di resilienza a livello di Unione e dei relativi risultati.

6. Il gruppo di cooperazione NIS, in collaborazione con la Commissione, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza («alto rappresentante») e l'ENISA e, nell'ambito del suo mandato, EU-CyCLONe, elabora scenari di rischio e metodologie comuni per la verifica coordinata della preparazione a norma dell'articolo 11, lettera a), punto i), e, se del caso, per altre azioni di preparazione a norma della lettera a), punto ii), di tale articolo.

7. Quando un soggetto che opera in un settore ad alta criticità partecipa volontariamente alla verifica coordinata della preparazione e tale verifica dà luogo a raccomandazioni per misure specifiche, che il soggetto partecipante potrebbe integrare in un piano di ripristino, l'autorità dello Stato membro responsabile della verifica coordinata della preparazione riesamina, se del caso, il seguito dato a tali misure dai soggetti partecipanti al fine di rafforzare la preparazione.

Articolo 13

Altre azioni di preparazione

1. Il meccanismo per le emergenze di cibersicurezza sostiene azioni di preparazione non contemplate dall'articolo 12. Tali azioni comprendono azioni di preparazione per i soggetti in settori non individuati per la verifica coordinata di preparazione a norma dell'articolo 12. Tali azioni possono sostenere il monitoraggio delle vulnerabilità, il monitoraggio dei rischi, gli esercizi e la formazione.

2. Il sostegno alle azioni di preparazione di cui al presente articolo è fornito agli Stati membri su richiesta e principalmente sotto forma di sovvenzioni e alle condizioni previste nei pertinenti programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694.

Articolo 14

Istituzione della riserva dell'UE per la cibersicurezza

1. È istituita una riserva dell'UE per la cibersicurezza al fine di assistere, su richiesta, gli utenti di cui al paragrafo 3 nella risposta o nella fornitura di sostegno per la risposta agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e nell'avvio della ripresa da tali incidenti.

2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta erogati da fornitori di fiducia di servizi di sicurezza gestiti selezionati in base ai criteri di cui all'articolo 17, paragrafo 2. La riserva dell'UE per la cibersicurezza può includere servizi preimpegnati. I servizi preimpegnati di un prestatore di fiducia di servizi di sicurezza gestiti sono convertibili in servizi di preparazione relativi alla prevenzione e alla risposta agli incidenti nei casi in cui tali servizi non siano utilizzati per la risposta agli incidenti durante il periodo per il quale sono preimpegnati. La riserva dell'UE per la cibersicurezza è mobilitabile su richiesta in tutti gli Stati membri, nelle istituzioni, negli organi e negli organismi dell'Unione e nei paesi terzi associati al programma Europa digitale di cui all'articolo 19, paragrafo 1.

3. Gli utenti che usufruiscono dei servizi forniti dalla riserva dell'UE per la cibersicurezza sono i seguenti:

a) le autorità di gestione delle crisi informatiche e i CSIRT degli Stati membri di cui rispettivamente all'articolo 9, paragrafi 1 e 2, e all'articolo 10 della direttiva (UE) 2022/2555;

b) CERT-UE conformemente all'articolo 13 del regolamento (UE, Euratom) 2023/2841;

c) le autorità competenti, quali i gruppi di intervento per la sicurezza informatica in caso di incidente e le autorità di gestione delle crisi informatiche dei paesi terzi associati al programma Europa digitale, conformemente all'articolo 19, paragrafo 8.

4. La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza. La Commissione determina le priorità e l'evoluzione della riserva dell'UE per la cibersicurezza in coordinamento con il gruppo di cooperazione NIS e in linea con i requisiti degli utenti di cui al paragrafo 3, ne supervisiona l'attuazione e assicura la complementarità, la coerenza, le sinergie e i collegamenti con altre azioni di sostegno ai sensi del presente regolamento,

nonché con altre azioni e programmi dell'Unione. Tali priorità sono riesaminate e, se del caso, rivedute ogni due anni. La Commissione informa il Parlamento europeo e il Consiglio in merito a tali priorità e alla loro eventuale revisione.

5. Fatta salva la responsabilità generale della Commissione per l'attuazione della riserva dell'UE per la cibersicurezza di cui al paragrafo 4 del presente articolo e fatto salvo un accordo di contributo quale definito all'articolo 2, punto 19), del regolamento (UE, Euratom) 2024/2509, la Commissione affida all'ENISA, in tutto o in parte, il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza. Gli aspetti non affidati all'ENISA restano soggetti alla gestione diretta da parte della Commissione.

6. L'ENISA prepara, almeno ogni due anni, una mappatura dei servizi necessari agli utenti di cui al paragrafo 3, lettere a) e b), del presente articolo. La mappatura include anche la disponibilità di tali servizi, anche presso soggetti giuridici stabiliti o ritenuti stabiliti negli Stati membri e controllati da Stati membri o da cittadini degli Stati membri. Nel mappare tale disponibilità, l'ENISA valuta le competenze e le capacità della forza lavoro dell'Unione nel settore della cibersicurezza pertinenti per gli obiettivi della riserva dell'UE per la cibersicurezza. Nel preparare la mappatura, l'ENISA consulta il gruppo di cooperazione NIS, EU-CyCLONe, la Commissione e, se del caso, il comitato interistituzionale per la cibersicurezza (Interinstitutional Cybersecurity Board - IICB) istituito a norma dell'articolo 10 del regolamento (UE, Euratom) 2023/2841. Nel mappare la disponibilità dei servizi, l'ENISA consulta anche i pertinenti portatori di interessi del settore della cibersicurezza, compresi i fornitori di servizi di sicurezza gestiti. L'ENISA prepara una mappatura analoga, dopo aver informato il Consiglio e previa consultazione con EU-CyCLONe, con la Commissione e, se del caso, con l'alto rappresentante, al fine di individuare le esigenze degli utenti di cui al paragrafo 3, lettera c), del presente articolo.

7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 23 al fine di integrare il presente regolamento specificando i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza. Nella preparazione di tali atti delegati, la Commissione tiene conto della mappatura di cui al paragrafo 6 del presente articolo e può scambiare pareri e cooperare con il gruppo di cooperazione NIS e l'ENISA.

Articolo 15

Richieste di sostegno della riserva dell'UE per la cibersicurezza

1. Gli utenti di cui all'articolo 14, paragrafo 3, possono richiedere servizi della riserva dell'UE per la cibersicurezza a sostegno della risposta agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e per avviare la ripresa dagli stessi.

2. Per ricevere il sostegno della riserva dell'UE per la cibersicurezza, gli utenti di cui all'articolo 14, paragrafo 3, adottano tutte le misure adeguate per attenuare gli effetti dell'incidente per il quale è richiesto il sostegno, compresa, se del caso, la fornitura di assistenza tecnica diretta e di altre risorse volte a sostenere la risposta all'incidente e gli sforzi di ripresa.

3. Le richieste di sostegno sono trasmesse all'amministrazione aggiudicatrice come segue:

a) nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera a), del presente regolamento, tramite il punto di contatto unico designato o istituito a norma dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555;

b) nel caso dell'utente di cui all'articolo 14, paragrafo 3, lettera b), da tale utente;

c) nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera c), tramite il punto di contatto unico di cui all'articolo 19, paragrafo 9.

4. In caso di richieste da parte degli utenti di cui all'articolo 14, paragrafo 3, lettera a), gli Stati membri informano la rete di CSIRT e, se del caso, EU-CyCLONe in merito alle richieste di sostegno dei loro utenti nella risposta agli incidenti e nella ripresa iniziale ai sensi del presente articolo.

5. Le richieste di sostegno nella risposta agli incidenti e nella ripresa iniziale includono:

a) adeguate informazioni sul soggetto interessato e sugli impatti potenziali dell'incidente su:

   i) nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera a), gli Stati membri e gli utenti interessati, compreso il rischio di propagazione a un altro Stato membro;

ii) nel caso dell'utente di cui all'articolo 14, paragrafo 3, lettera b), le istituzioni, gli organi e gli organismi dell'Unione interessati;

iii) nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera c), i paesi associati al programma Europa digitale interessati;

b) informazioni sul servizio richiesto, unitamente all'uso previsto del sostegno richiesto, compresa un'indicazione delle esigenze stimate;

c) informazioni adeguate sulle misure adottate per attenuare l'impatto dell'incidente per il quale è richiesto il sostegno, di cui al paragrafo 2;

d) ove opportuno, informazioni disponibili su altre forme di sostegno disponibili per il soggetto interessato.

6. L'ENISA, in collaborazione con la Commissione e EU-CyCLONe, elabora un modello per facilitare la presentazione di richieste di sostegno della riserva dell'UE per la cibersicurezza.

7. La Commissione può specificare ulteriormente, mediante atti di esecuzione, le modalità procedurali dettagliate per il modo in cui i servizi di sostegno della riserva dell'UE per la cibersicurezza debbano essere richiesti ed le modalità tramite le quali a tali richieste debba essere data una risposta a norma del presente articolo, dell'articolo 16, paragrafo 1, e dell'articolo 19, paragrafo 10, comprese le modalità di presentazione di tali richieste e di trasmissione delle risposte e dei modelli per le relazioni di cui all'articolo 16, paragrafo 9. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 24, paragrafo 2.

Articolo 16

Attuazione del sostegno della riserva dell'UE per la cibersicurezza

1. Nel caso di richieste degli utenti di cui all'articolo 14, paragrafo 3, lettere a) e b), le richieste di sostegno della riserva dell'UE per la cibersicurezza sono valutate dall'amministrazione aggiudicatrice. Una risposta è trasmessa agli utenti di cui all'articolo 14, paragrafo 3, lettere a) e b), senza ritardo e in ogni caso entro 48 ore dalla presentazione della richiesta per garantire l'efficacia del sostegno. L'amministrazione aggiudicatrice informa il Consiglio e la Commissione dei risultati della procedura.

2. Per quanto riguarda le informazioni condivise nel corso della richiesta e della fornitura dei servizi della riserva dell'UE per la cibersicurezza, tutte le parti coinvolte nell'applicazione del presente regolamento:

a) limitano l'uso e la condivisione di tali informazioni a quanto necessario per adempiere ai propri obblighi o funzioni ai sensi del presente regolamento;

b) utilizzano e condividono le informazioni riservate o classificate a norma del diritto dell'Unione e nazionale solo in conformità di tale diritto; e

c) assicurano uno scambio di informazioni efficace, efficiente e sicuro, se del caso utilizzando e rispettando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP.

3. Nel valutare le singole richieste ai sensi dell'articolo 16, paragrafo 1 e dell'articolo 19, paragrafo 10, l'amministrazione aggiudicatrice o la Commissione, a seconda dei casi, valuta innanzitutto se i criteri di cui all'articolo 15, paragrafi 1 e 2, sono soddisfatti. In caso positivo, l'amministrazione aggiudicatrice o la Commissione valuta l'adeguatezza della durata e della natura del sostegno tenendo conto dell'obiettivo di cui all'articolo 1, paragrafo 3, lettera b), e, se del caso, dei criteri seguenti:

a) la portata e la gravità dell'incidente;

b) il tipo di soggetto interessato, dando maggiore priorità agli incidenti che colpiscono soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555;

c) l'impatto potenziale dell'incidente sugli Stati membri, sulle istituzioni, sugli organi o sugli organismi dell'Unione o sui paesi terzi associati al programma Europa digitale interessati;

d) la natura potenzialmente transfrontaliera dell'incidente e il rischio di propagazione ad altri Stati membri, istituzioni, organi od organismi dell'Unione o paesi terzi associati al programma Europa digitale;

e) le misure adottate dall'utente per sostenere la risposta e gli sforzi di ripresa iniziali, di cui all'articolo 15, paragrafo 2.

4. Per definire l'ordine di priorità delle richieste, in caso di richieste concomitanti da parte degli utenti di cui all'articolo 14, paragrafo 3, si tiene conto, se del caso, dei criteri di cui al paragrafo 3 del presente articolo, fatto salvo il principio di leale cooperazione tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. Qualora due o più richieste siano considerate equivalenti in base a tali criteri, è data maggiore priorità alle richieste degli utenti degli Stati membri. Qualora il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza siano stati affidati, in tutto o in parte, all'ENISA a norma dell'articolo 14, paragrafo 5, l'ENISA e la Commissione cooperano strettamente per dare priorità alle richieste in conformità del presente paragrafo.

5. I servizi della riserva dell'UE per la cibersicurezza sono forniti in conformità di accordi specifici stipulati tra il fornitore di fiducia di servizi di sicurezza gestiti e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE per la cibersicurezza. Tali servizi possono essere forniti conformemente ad accordi specifici tra il fornitore di fiducia di servizi di sicurezza gestiti, l'utente e l'entità interessata. Tutti gli accordi di cui al presente paragrafo includono, tra l'altro, condizioni di responsabilità.

6. Gli accordi di cui al paragrafo 5 sono basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri e, ove opportuno, di altri utenti della riserva dell'UE per la cibersicurezza.

7. La Commissione, l'ENISA e gli utenti della riserva dell'UE per la cibersicurezza non si assumono alcuna responsabilità contrattuale per i danni causati a terzi dai servizi forniti nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza.

8. Gli utenti possono utilizzare i servizi della riserva dell'UE per la cibersicurezza forniti in risposta a una richiesta a norma dell'articolo 15, paragrafo 1, solo per sostenere la risposta agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e per avviare la ripresa. Essi possono avvalersi di tali servizi solo per quanto riguarda:

a) soggetti che operano in settori ad alta criticità o soggetti che operano in altri settori critici, nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera a), e soggetti equivalenti nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera c); e

b) le istituzioni, gli organi e gli organismi dell'Unione, nel caso dell'utente di cui all'articolo 14, paragrafo 3, lettera b).

9. Entro due mesi dalla fine di un sostegno, gli utenti che hanno ricevuto sostegno forniscono una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti:

a) alla Commissione, all'ENISA, alla rete di CSIRT e a EU-CyCLONe nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera a);

b) alla Commissione, all'ENISA e all'IICB nel caso degli utenti di cui di cui all'articolo 14, paragrafo 3, lettera b);

c) alla Commissione nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera c).

La Commissione trasmette al Consiglio e all'alto rappresentante tutte le relazioni di sintesi ricevute dagli utenti di cui all'articolo 14, paragrafo 3, a norma del primo comma, lettera c), del presente paragrafo.

10. Qualora il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza siano stati affidati, in tutto o in parte, all'ENISA a norma dell'articolo 14, paragrafo 5, del presente regolamento, l'ENISA riferisce alla Commissione e la consulta al riguardo su base periodica. In tale contesto, l'ENISA invia immediatamente alla Commissione le richieste ricevute dagli utenti di cui all'articolo 14, paragrafo 3, lettera c), del presente regolamento e, se necessario ai fini della definizione delle priorità a norma del presente articolo, le richieste ricevute dagli utenti di cui all'articolo 14, paragrafo 3, lettera a) o b), del presente regolamento. Gli obblighi di cui al presente paragrafo lasciano impregiudicato l'articolo 14 del regolamento (UE) 2019/881.

11. Nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettere a) e b), l'amministrazione aggiudicatrice riferisce periodicamente e almeno due volte l'anno al gruppo di cooperazione NIS in merito alle modalità di impiego e ai risultati del sostegno.

12. Nel caso degli utenti di cui all'articolo 14, paragrafo 3, lettera c), la Commissione riferisce al Consiglio e informa l'alto rappresentante periodicamente e almeno due volte l'anno in merito alle modalità di impiego e ai risultati del sostegno.

Articolo 17

Fornitori di fiducia di servizi di sicurezza gestiti

1. Nelle procedure di appalto per l'istituzione della riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice agisce in conformità dei principi stabiliti nel regolamento (UE, Euratom) 2024/2509 e conformemente ai principi seguenti:

a) garantire che i servizi inclusi nella riserva dell'UE per la cibersicurezza, considerati nel loro insieme, siano tali per cui la riserva dell'UE per la cibersicurezza includa servizi che siano mobilitabili in tutti gli Stati membri, tenendo conto in particolare dei requisiti nazionali per la fornitura di tali servizi, tra l'altro in materia di lingue, certificazione o accreditamento;

b) garantire la protezione degli interessi essenziali di sicurezza dell'Unione e dei suoi Stati membri;

c) garantire che la riserva dell'UE per la cibersicurezza apporti valore aggiunto dell'Unione, contribuendo agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'Unione.

2. Al momento dell'appalto di servizi per la riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice include nei documenti di gara i criteri e i requisiti seguenti:

a) il fornitore dimostra che il suo personale è dotato della massima integrità professionale, indipendenza e responsabilità, nonché della competenza tecnica necessaria per svolgere le attività nel suo campo specifico, e garantisce la permanenza e continuità delle competenze e delle risorse tecniche necessarie;

b) il fornitore, nonché eventuali filiali e subappaltatori pertinenti, rispettano le norme applicabili in materia di protezione delle informazioni classificate e mettono in atto misure adeguate, compresi, se del caso, accordi conclusi tra di essi, per la protezione delle informazioni riservate relative al servizio, in particolare delle prove, dei risultati e delle relazioni;

c) il fornitore dimostra, tramite prove sufficienti, che la sua struttura di governo è trasparente, non suscettibile di compromettere la sua imparzialità e la qualità dei servizi prestati o di causare conflitti di interesse;

d) il fornitore è in possesso di un nulla osta di sicurezza adeguato, almeno per il personale destinato alla mobilitazione del servizio, laddove richiesto da uno Stato membro;

e) il fornitore dispone del livello di sicurezza pertinente per i suoi sistemi informatici;

f) il fornitore è dotato dell'hardware e del software necessari a supportare il servizio richiesto, che non contengono vulnerabilità sfruttabili note, includono gli ultimi aggiornamenti di sicurezza e rispettano in ogni caso le disposizioni applicabili del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio ([23]);

g) il fornitore è in grado di dimostrare di avere esperienza nella fornitura di servizi analoghi alle autorità nazionali competenti, ai soggetti che operano in settori ad alta criticità o ai soggetti che operano in altri settori critici;

h) il fornitore è in grado di prestare il servizio in tempi brevi negli Stati membri in cui può fornire il servizio;

i) il fornitore è in grado di prestare il servizio in una o più lingue ufficiali delle istituzioni dell'Unione o di uno Stato membro come richiesto, se del caso, dagli Stati membri o dagli utenti di cui all'articolo 14, paragrafo 3, lettere b) e c), a cui il fornitore può fornire il servizio;

j) una volta posto in essere un sistema europeo di certificazione della cibersicurezza per i servizi di sicurezza gestiti a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema entro due anni dalla data di applicazione del sistema;

([23]) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

k) il fornitore include nell'offerta le condizioni di conversione per eventuali servizi di risposta agli incidenti non utilizzati che potrebbero essere convertiti in servizi di preparazione strettamente connessi alla risposta agli incidenti, quali esercitazioni o formazioni.

3. Ai fini dell'appalto di servizi per la riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice, se del caso, può definire criteri e requisiti aggiuntivi rispetto a quelli di cui al paragrafo 2, in stretta collaborazione con gli Stati membri.

Articolo 18

Azioni a sostegno dell'assistenza reciproca

1. Il meccanismo per le emergenze di cibersicurezza fornisce sostegno per l'assistenza tecnica prestata da uno Stato membro a un altro Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o un incidente di cibersicurezza su vasta scala, anche nei casi di cui all'articolo 11, paragrafo 3, lettera f), della direttiva (UE) 2022/2555.

2. Il sostegno per l'assistenza tecnica reciproca di cui al paragrafo 1 del presente articolo è fornito sotto forma di sovvenzioni e alle condizioni previste nei pertinenti programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694.

Articolo 19

Sostegno ai paesi terzi associati al programma Europa digitale

1. Un paese terzo associato al programma Europa digitale può richiedere il sostegno della riserva dell'UE per la cibersicurezza se l'accordo attraverso cui è associato al programma Europa digitale prevede la partecipazione alla riserva dell'UE per la cibersicurezza. Tale accordo include disposizioni che impongono al paese terzo associato al programma Europa digitale interessato di rispettare gli obblighi di cui ai paragrafi 2 e 9 del presente articolo. Ai fini della partecipazione di un paese terzo alla riserva dell'UE per la cibersicurezza, l'associazione parziale di un paese terzo al programma Europa digitale può comprendere un'associazione limitata all'obiettivo operativo di cui all'articolo 6, paragrafo 1, lettera g), del regolamento (UE) 2021/694.

2. Entro tre mesi dalla conclusione dell'accordo di cui al paragrafo 1 e in ogni caso prima di ricevere il sostegno della riserva dell'UE per la cibersicurezza, il paese terzo associato al programma Europa digitale fornisce alla Commissione informazioni sulle proprie capacità di resilienza informatica e di gestione del rischio, tra cui almeno le informazioni sulle misure nazionali adottate per prepararsi agli incidenti di cibersicurezza significativi o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala, nonché informazioni sui soggetti nazionali responsabili, compresi i gruppi di intervento per la sicurezza informatica in caso di incidente o soggetti equivalenti, sulle loro capacità e sulle risorse loro assegnate. Il paese terzo associato al programma Europa digitale fornisce aggiornamenti di tali informazioni su base periodica e almeno una volta all'anno. La Commissione fornisce tali informazioni all'alto rappresentante e all'ENISA al fine di agevolare l'applicazione del paragrafo 11.

3. La Commissione valuta periodicamente, e almeno una volta all'anno, i seguenti criteri per ciascun paese terzo associato al programma Europa digitale di cui al paragrafo 1:

a) se il paese rispetta le condizioni dell'accordo di cui al paragrafo 1 nella misura in cui esse si riferiscono alla partecipazione alla riserva dell'UE per la cibersicurezza;

b) se il paese ha adottato misure adeguate per prepararsi a incidenti di cibersicurezza significativi o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala, sulla base delle informazioni di cui al paragrafo 2; e

c) se il sostegno fornito è coerente con la politica dell'Unione nei confronti del paese e con le sue relazioni generali con il paese, e se è coerente con altre politiche dell'Unione in materia di sicurezza.

Nell'effettuare la valutazione di cui al primo comma, la Commissione consulta l'alto rappresentante per quanto riguarda il criterio di cui alla lettera c) dello stesso comma.

Se conclude che un paese terzo associato al programma Europa digitale soddisfa tutte le condizioni di cui al primo comma, la Commissione presenta al Consiglio una proposta di adozione di un atto di esecuzione conformemente al paragrafo 4 per autorizzare la fornitura di sostegno a titolo della riserva dell'UE per la cibersicurezza nei confronti di tale paese.

4. Il Consiglio può adottare gli atti di esecuzione di cui al paragrafo 3. Tali atti di esecuzione si applicano al massimo per un anno, sono rinnovabili e possono prevedere un limite, non inferiore a 75 giorni, per il numero di giorni per i quali può essere fornito sostegno in risposta a un'unica richiesta.

Ai fini del presente articolo il Consiglio agisce rapidamente e, di norma, adotta gli atti di esecuzione di cui al presente paragrafo entro otto settimane dall'adozione della pertinente proposta della Commissione a norma del paragrafo 3, terzo comma.

5. Il Consiglio può modificare o abrogare un atto di esecuzione adottato a norma del paragrafo 4 in qualsiasi momento, su proposta della Commissione.

Qualora ritenga che vi sia stato un cambiamento significativo per quanto riguarda il criterio di cui al paragrafo 3, primo comma, lettera c), il Consiglio può modificare o abrogare un atto di esecuzione adottato a norma del paragrafo 4 su iniziativa debitamente motivata di uno o più Stati membri.

6. Nell'esercizio delle sue competenze di esecuzione a norma del presente articolo, il Consiglio applica i criteri di cui al paragrafo 3, primo comma, e spiega la sua valutazione di tali criteri. In particolare, quando agisce di propria iniziativa a norma del paragrafo 5, secondo comma, il Consiglio illustra il cambiamento significativo di cui a tale comma.

7. Il sostegno della riserva dell'UE per la cibersicurezza a un paese terzo associato al programma Europa digitale è conforme alle condizioni specifiche stabilite nell'accordo di cui al paragrafo 1.

8. Tra gli utenti dei paesi terzi associati al programma Europa digitale che possono essere destinatari dei servizi della riserva dell'UE per la cibersicurezza rientrano le autorità competenti come i gruppi di intervento per la sicurezza informatica in caso di incidente o soggetti equivalenti e le autorità di gestione delle crisi informatiche.

9. Ogni paese terzo associato al programma Europa digitale ammissibile al sostegno della riserva dell'UE per la cibersicurezza designa un'autorità che funga da punto di contatto unico ai fini del presente regolamento.

10. Le richieste di sostegno a titolo della riserva dell'UE per la cibersicurezza a norma del presente articolo sono valutate dalla Commissione. L'amministrazione aggiudicatrice può fornire sostegno a un paese terzo solo se e nella misura in cui è in vigore un atto di esecuzione del Consiglio che autorizza il sostegno in relazione a tale paese, adottato conformemente al paragrafo 4 del presente articolo. Una risposta è trasmessa senza indebito ritardo agli utenti di cui all'articolo 14, paragrafo 3, lettera c).

11. Quando riceve una richiesta di sostegno a norma del presente articolo, la Commissione ne informa immediatamente il Consiglio. La Commissione tiene informato il Consiglio in merito alla valutazione della richiesta. La Commissione collabora altresì con l'alto rappresentante in merito alle richieste ricevute e all'attuazione del sostegno concesso ai paesi terzi associati al programma Europa digitale dalla riserva dell'UE per la cibersicurezza. Inoltre la Commissione tiene anche conto di eventuali pareri forniti dall'ENISA in merito a tali richieste.

Articolo 20

Coordinamento con i meccanismi di gestione delle crisi dell'Unione

1. Se un incidente di cibersicurezza significativo, un incidente di cibersicurezza su vasta scala o un incidente di cibersicurezza equivalente a incidenti su vasta scala è causato da una catastrofe quale definita all'articolo 4, punto 1), della decisione n. 1313/2013/UE, o dà luogo a una catastrofe, il sostegno previsto dal presente regolamento per rispondere a tale incidente integra le azioni di cui alla decisione n. 1313/2013/UE senza pregiudicare quest'ultima.

2. Nel caso di un incidente di cibersicurezza su vasta scala o di un incidente di cibersicurezza equivalente a incidenti su vasta scala che comporti l'attivazione dei dispositivi integrati dell'UE per la risposta politica alle crisi (Integrated Political Crisis Response Arrangements - IPCR) di cui alla decisione di esecuzione (UE) 2018/1993 (dispositivi IPCR), il sostegno previsto dal presente regolamento per rispondere a tale incidente è gestito in conformità delle apposite procedure nell'ambito dei dispositivi IPCR.

CAPO IV

MECCANISMO EUROPEO DI RIESAME DEGLI INCIDENTI DI CIBERSICUREZZA

Articolo 21

Meccanismo europeo di riesame degli incidenti di cibersicurezza

1. Su richiesta della Commissione o di EU-CyCLONe, l'ENISA, con il sostegno della rete di CSIRT e con l'approvazione degli Stati membri interessati, riesamina e valuta le minacce informatiche, le vulnerabilità sfruttabili note e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o incidente di cibersicurezza su vasta scala. Al termine del riesame e della valutazione di un incidente e al fine di trarre gli opportuni insegnamenti per evitare o attenuare futuri incidenti, l'ENISA presenta una relazione di riesame dell'incidente a EU-CyCLONe, alla rete di CSIRT, agli Stati membri interessati e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare quelli stabiliti agli articoli 15 e 16 della direttiva (UE) 2022/2555. Qualora un incidente abbia un impatto su un paese terzo associato al programma Europa digitale, l'ENISA fornisce la relazione al Consiglio. In tali casi, la Commissione fornisce la relazione all'alto rappresentante.

2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1 del presente articolo, l'ENISA coopera con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, la Commissione, altre istituzioni e altri organi e organismi pertinenti dell'Unione, l'industria, inclusi i fornitori di servizi di sicurezza gestiti, e gli utenti di servizi di cibersicurezza, e raccoglie i feedback da essi ricevuti. Ove opportuno, l'ENISA, in collaborazione con i CSIRT e, se del caso, le autorità competenti designate o stabilite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, coopera anche con i soggetti interessati da incidenti di cibersicurezza significativi o da incidenti di cibersicurezza su vasta scala. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.

3. La relazione di riesame dell'incidente di cui al paragrafo 1 del presente articolo comprende un riesame e un'analisi dello specifico incidente di cibersicurezza significativo o incidente di cibersicurezza su vasta scala, nonché delle cause principali, delle vulnerabilità sfruttabili note e degli insegnamenti tratti. L'ENISA assicura che la relazione sia conforme al diritto dell'Unione o nazionale in materia di protezione delle informazioni sensibili o classificate. Se richiesto dagli Stati membri interessati o altri utenti di cui all'articolo 14, paragrafo 3, che sono interessati dall'incidente, i dati e le informazioni contenuti nella relazione sono anonimizzati. La relazione non include dettagli sulle vulnerabilità sfruttate attivamente che rimangono non risolte.

4. Ove opportuno, la relazione di riesame dell'incidente formula raccomandazioni per migliorare la posizione dell'Unione in materia di deterrenza informatica e può includere le migliori pratiche e gli insegnamenti tratti dai portatori di interessi.

5. L'ENISA può fornire una versione pubblica della relazione di riesame dell'incidente. Tale versione della relazione contiene solo informazioni pubbliche affidabili o altre informazioni affidabili per cui è stato ottenuto il consenso degli Stati membri interessati e, per quanto riguarda le informazioni relative a un utente di cui all'articolo 14, paragrafo 3, lettere b) o c), il consenso di tale utente.

CAPO V

DISPOSIZIONI FINALI

Articolo 22

Modifiche del regolamento (UE) 2021/694

Il regolamento (UE) 2021/694 è così modificato:

1) l'articolo 6 è così modificato:

a) il paragrafo 1 è così modificato:

i) è inserita la seguente lettera:

«a *bis*) sostenere lo sviluppo del sistema europeo di allerta per la cibersicurezza istituito dall'articolo 3 del regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio (*) ("sistema europeo di allerta per la cibersicurezza"), compresi l'elaborazione, la realizzazione e il funzionamento di poli informatici nazionali e poli informatici transfrontalieri che contribuiscano alla conoscenza situazionale nell'Unione e al potenziamento delle capacità di analisi delle minacce informatiche dell'Unione;

(*) Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).»;

ii) è aggiunta la lettera seguente:

«g) istituire e gestire il meccanismo per le emergenze di cibersicurezza istituito dall'articolo 10 del regolamento (UE) 2025/38, che comprende la riserva dell'UE per la cibersicurezza istituita dall'articolo 14 di tale regolamento ("riserva dell'UE per la cibersicurezza"), inteso a sostenere gli Stati membri nella preparazione agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala e nella risposta agli stessi, a integrazione delle risorse e delle capacità nazionali e di altre forme di sostegno disponibili a livello di Unione, e inteso a sostenere gli altri utenti nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala.»;

b) il paragrafo 2 è sostituito dal seguente:

«2. Le azioni nell'ambito dell'obiettivo specifico 3 sono attuate principalmente mediante il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento in conformità del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio (*). Tuttavia, la riserva dell'UE per la cibersicurezza è attuata dalla Commissione e, in conformità dell'articolo 14, paragrafo 6, del regolamento (UE) 2025/38, dall'ENISA.;

(*) Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento (GU L 202 dell'8.6.2021, pag. 1).».

2) l'articolo 9 è così modificato:

a) al paragrafo 2, le lettere b), c) e d) sono sostituite dalle seguenti:

«b) 1 760 806 000 EUR per l'obiettivo specifico 2 — Intelligenza artificiale;

c) 1 372 020 000 EUR per l'obiettivo specifico 3 — Cibersicurezza e fiducia;

d) 482 640 000 EUR per l'obiettivo specifico 4 — Competenze digitali avanzate;»;

b) è aggiunto il seguente paragrafo:

«8. In deroga all'articolo 12, paragrafo 1, del regolamento finanziario, gli stanziamenti d'impegno e di pagamento non utilizzati per le azioni nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza e le azioni a sostegno dell'assistenza reciproca a norma del regolamento (UE) 2025/38 che perseguono gli obiettivi di cui all'articolo 6, paragrafo 1, lettera g), del presente regolamento sono riportati di diritto e possono essere impegnati e pagati fino al 31 dicembre dell'esercizio successivo. Il Parlamento europeo e il Consiglio sono informati degli stanziamenti riportati a norma dell'articolo 12, paragrafo 6, del regolamento finanziario.»;

3) l'articolo 12 è così modificato:

a) sono inseriti i paragrafi seguenti:

«5 *bis*. Il paragrafo 5 non si applica, per quanto riguarda i soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi, a qualsiasi azione di attuazione del sistema europeo di allerta per la cibersicurezza se entrambe le condizioni seguenti sono soddisfatte in relazione all'azione interessata:

a) esiste un rischio reale, alla luce dei risultati della mappatura effettuata a norma dell'articolo 9, paragrafo 4, del regolamento (UE) 2025/38, che gli strumenti, le infrastrutture o i servizi necessari e sufficienti affinché tale azione contribuisca in modo adeguato all'obiettivo del sistema europeo di allerta per la cibersicurezza non siano disponibili presso i soggetti giuridici stabiliti o considerati stabiliti negli Stati membri e controllati da Stati membri o da cittadini di Stati membri;

b) il rischio per la sicurezza derivante dall'approvvigionamento presso tali soggetti giuridici nell'ambito del sistema europeo di allerta per la cibersicurezza è proporzionato ai benefici e non compromette gli interessi essenziali di sicurezza dell'Unione e dei suoi Stati membri.

5 *ter*. Il paragrafo 5 non si applica, per quanto riguarda i soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi, alle eventuali azioni di attuazione della riserva dell'UE per la cibersicurezza se entrambe le condizioni seguenti sono soddisfatte con riguardo all'azione interessata:

a) esiste un rischio reale, alla luce dei risultati della mappatura di cui effettuata a norma dell'articolo 14, paragrafo 7, del regolamento (UE) 2025/38, che la tecnologia, le competenze o la capacità necessarie e sufficienti affinché la riserva dell'UE per la cibersicurezza svolga adeguatamente le sue funzioni non siano disponibili presso i soggetti giuridici stabiliti o considerati stabiliti negli Stati membri e controllati da Stati membri o da cittadini di Stati membri;

b) il rischio per la sicurezza derivante dall'inclusione di tali soggetti giuridici nell'ambito della riserva dell'UE per la cibersicurezza è proporzionato ai benefici e non compromette gli interessi essenziali di sicurezza dell'Unione e dei suoi Stati membri.»;

b) il paragrafo 6 è sostituito dal seguente:

«6. Se debitamente giustificato per ragioni di sicurezza, il programma di lavoro può prevedere altresì che i soggetti giuridici stabiliti in paesi associati e i soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi siano ammessi a partecipare a tutte o ad alcune delle azioni nell'ambito degli obiettivi specifici 1 e 2 unicamente se soddisfano i requisiti che tali soggetti giuridici devono soddisfare per garantire la tutela degli interessi essenziali di sicurezza dell'Unione e degli Stati membri e per assicurare la protezione delle informazioni di documenti classificati. Tali requisiti sono definiti nel programma di lavoro.

Il primo comma si applica anche, per quanto riguarda i soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi, alle azioni nell'ambito dell'obiettivo specifico 3:

a) volte ad attuare il sistema europeo di allerta per la cibersicurezza nei casi in cui si applica il paragrafo 5 *bis*; e

b) volte ad attuare la riserva dell'UE per la cibersicurezza nei casi in cui si applica il paragrafo 5 *ter*.»;

4) all'articolo 14, il paragrafo 2 è sostituito dal seguente:

«2. Il Programma può concedere finanziamenti in tutte le forme previste dal regolamento finanziario, anche, in particolare, sotto forma di appalti, quale forma principale, o di sovvenzioni e premi.

Qualora, per il conseguimento di uno degli obiettivi di un'azione, siano necessarie gare di appalto per acquisire beni e servizi innovativi, le sovvenzioni possono essere concesse unicamente a beneficiari che sono amministrazioni aggiudicatrici o enti aggiudicatori ai sensi delle direttive 2014/24/UE (*) e 2014/25/UE (**) del Parlamento europeo e del Consiglio.

Qualora la fornitura di beni o servizi innovativi non ancora disponibili su larga scala commerciale sia necessaria per il conseguimento degli obiettivi di un'azione, l'amministrazione aggiudicatrice o l'ente aggiudicatore può autorizzare l'aggiudicazione di contratti multipli nell'ambito della stessa procedura di appalto.

Per motivi di pubblica sicurezza debitamente giustificati, l'amministrazione aggiudicatrice o l'ente aggiudicatore può imporre come condizione che il luogo di esecuzione del contratto sia situato nel territorio dell'Unione.

Nell'attuazione delle procedure di appalto per la riserva dell'UE per la cibersicurezza, la Commissione e l'ENISA possono fungere da centrale di committenza per condurre una procedura di appalto per conto o a nome di paesi terzi associati al Programma in conformità dell'articolo 10 del presente regolamento. La Commissione e l'ENISA possono anche agire in veste di grossisti, comprando, immagazzinando e rivendendo o donando forniture e servizi, comprese le locazioni, per

tali paesi terzi. In deroga all'articolo 169, paragrafo 3, del regolamento (UE, Euratom) 2024/2509 del Parlamento Europeo e del Consiglio (***), la richiesta di un singolo paese terzo è sufficiente per conferire alla Commissione o all'ENISA il mandato di agire.

Nell'attuazione delle procedure di appalto per la riserva dell'UE per la cibersicurezza, la Commissione e l'ENISA possono fungere da centrale di committenza per condurre una procedura di appalto per conto o a nome di istituzioni, organi o organismi dell'Unione. La Commissione e l'ENISA possono anche agire in veste di grossisti, comprando, immagazzinando e rivendendo o donando forniture e servizi, comprese le locazioni, per le istituzioni, gli organi o gli organismi dell'Unione. In deroga all'articolo 168, paragrafo 3, del regolamento (UE, Euratom) 2024/2509, una richiesta di una singola istituzione o di un singolo organo o organismo dell'Unione è sufficiente per conferire alla Commissione o all'ENISA il mandato di agire.

Il Programma può inoltre concedere finanziamenti sotto forma di strumenti finanziari nell'ambito di operazioni di finanziamento misto.

(*) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).
(**) Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE (GU L 94 del 28.3.2014, pag. 243).
(***) Regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio, del 23 settembre 2024, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione (GU L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).»;

5) è inserito l'articolo seguente:

«*Articolo 16 bis*

Conflitto tra norme

Nel caso di azioni volte ad attuare il sistema europeo di allerta per la cibersicurezza, le norme applicabili sono quelle sancite agli articoli 4, 5 e 9 del regolamento (UE) 2025/38. In caso di conflitto tra le disposizioni del presente regolamento e gli articoli 4, 5 e 9 del regolamento (UE) 2025/38 prevalgono questi ultimi e si applicano a tali azioni specifiche.

Nel caso della riserva dell'UE per la cibersicurezza, norme specifiche per la partecipazione di paesi terzi associati al programma sono stabilite all'articolo 19 del regolamento (UE) 2025/38. In caso di conflitto tra le disposizioni del presente regolamento e l'articolo 19 del regolamento (UE) 2025/38 prevale quest'ultimo e si applica a tali azioni specifiche.»;

6) l'articolo 19 è sostituito dal seguente:

«*Articolo 19*

Sovvenzioni

Le sovvenzioni nell'ambito del Programma sono attribuite e gestite conformemente al titolo VIII del regolamento finanziario e possono coprire fino al 100 % dei costi ammissibili, fatto salvo il principio di cofinanziamento stabilito all'articolo 190 del regolamento finanziario. Tali sovvenzioni devono essere concesse e gestite conformemente a ciascun obiettivo specifico.

Il sostegno erogato sotto forma di sovvenzioni può essere concesso direttamente dall'ECCC, senza invito a presentare proposte, agli Stati membri selezionati a norma dell'articolo 9 del regolamento (UE) 2025/38, e al consorzio ospitante di cui all'articolo 5 del regolamento (UE) 2025/38, in conformità dell'articolo 195, primo comma, lettera d), del regolamento finanziario.

Il sostegno erogato sotto forma di sovvenzioni per il meccanismo per le emergenze di cibersicurezza può essere concesso direttamente dall'ECCC agli Stati membri senza invito a presentare proposte, in conformità dell'articolo 195, primo comma, lettera d), del regolamento finanziario.

Per quanto riguarda le azioni a sostegno dell'assistenza reciproca di cui all'articolo 18 del regolamento (UE) 2025/38, l'ECCC informa la Commissione e l'ENISA sulle richieste di sovvenzioni dirette degli Stati membri senza invito a presentare proposte.

Per quanto riguarda le azioni a sostegno dell'assistenza reciproca di cui all'articolo 18 del regolamento (UE) 2025/38, e in conformità dell'articolo 193, paragrafo 2, secondo comma, lettera a), del regolamento finanziario, in casi debitamente giustificati i costi possono essere considerati ammissibili anche se sono stati sostenuti prima della presentazione della domanda di sovvenzione.»;

7) gli allegati I e II sono modificati conformemente all'allegato del presente regolamento.

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 14, paragrafo 7, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 5 febbraio 2025. 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 14, paragrafo 7, 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 14, paragrafo 7, 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 dal comitato di coordinamento del programma Europa digitale di cui all'articolo 31, paragrafo 1, del regolamento (UE) 2021/694. 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.

Articolo 25

Valutazione e riesame

1. Entro il 5 febbraio 2027 e successivamente almeno ogni quattro anni, la Commissione valuta il funzionamento delle misure di cui al presente regolamento e trasmette al Parlamento europeo e al Consiglio una relazione.

2. La valutazione di cui al paragrafo 1 considera in particolare gli elementi seguenti:

a) il numero di poli informatici nazionali e di poli informatici transfrontalieri istituiti, la portata delle informazioni condivise, compreso se possibile l'impatto sul lavoro della rete di CSIRT, e la misura in cui tali poli hanno contribuito a rafforzare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici e a sviluppare tecnologie all'avanguardia; l'uso dei finanziamenti del programma Europa digitale per gli strumenti, le infrastrutture o i servizi di cibersicurezza acquisiti congiuntamente; e, se sono disponibili informazioni al riguardo, il

livello di cooperazione tra i poli informatici nazionali e le comunità settoriali e intersettoriali di soggetti essenziali e importanti di cui all'articolo 3 della direttiva (UE) 2022/2555;

b) l'uso e l'efficacia delle azioni a sostegno della preparazione nell'ambito del meccanismo per le emergenze di cibersicurezza, compresa la formazione, la risposta agli incidenti di cibersicurezza significativi, agli incidenti di cibersicurezza su vasta scala e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala e la ripresa iniziale dagli stessi, tra cui l'uso dei finanziamenti del programma Europa digitale e gli insegnamenti tratti e le raccomandazioni derivanti dall'attuazione del meccanismo per le emergenze di cibersicurezza;

c) l'uso e l'efficacia della riserva dell'UE per la cibersicurezza in relazione ai tipi di utenti, compreso l'uso dei finanziamenti del programma Europa digitale, la diffusione dei servizi, compreso il loro tipo, il tempo medio di risposta alle richieste e di mobilitazione della riserva dell'UE per la cibersicurezza, la percentuale di servizi convertiti in servizi di preparazione relativi alla prevenzione e alla risposta agli incidenti e gli insegnamenti tratti e le raccomandazioni derivanti dall'attuazione della riserva dell'UE per la cibersicurezza;

d) il contributo del presente regolamento al rafforzamento della posizione competitiva del settore industriale e di quello dei servizi nell'Unione nell'ambito dell'economia digitale, tra l'altro per le microimprese e le piccole e medie imprese nonché le start-up, e il contributo all'obiettivo generale di rafforzare le competenze e le capacità della forza lavoro in materia di cibersicurezza.

3. Sulla base delle relazioni di cui al paragrafo 1, la Commissione, se del caso, presenta una proposta legislativa al Parlamento europeo e al Consiglio al fine di modificare il presente regolamento.

Articolo 26

Entrata in vigore

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

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

Fatto a Bruxelles, il 19 dicembre 2024

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	BÓKA J.

ALLEGATO

Il regolamento (UE) 2021/694 è così modificato:

1) nell'allegato I, la sezione «Obiettivo specifico 3 — Cibersicurezza e fiducia» è sostituita dalla seguente:

«Obiettivo specifico 3 — Cibersicurezza e fiducia

Il Programma incentiva il rafforzamento, lo sviluppo e l'acquisizione di capacità essenziali volte a rendere sicure l'economia digitale, la società e la democrazia dell'Unione rafforzandone il potenziale industriale e la competitività in ambito di cibersicurezza, oltre a migliorare le capacità sia del settore privato sia del settore pubblico di proteggere i cittadini e le imprese dalle minacce informatiche, anche attraverso il sostegno all'attuazione della direttiva (UE) 2016/1148.

Le azioni iniziali e, laddove opportuno, le azioni successive del presente obiettivo comprendono:

1. il coinvestimento con gli Stati membri in attrezzature avanzate per la cibersicurezza, in infrastrutture e know-how, essenziali per proteggere le infrastrutture fondamentali e il mercato unico digitale nel suo complesso. Tale coinvestimento potrebbe comprendere investimenti in impianti quantistici e risorse di dati per la cibersicurezza e la conoscenza situazionale nel ciberspazio, compresi i poli informatici nazionali e i poli informatici transfrontalieri che costituiscono il sistema europeo di allerta per la cibersicurezza, e in altri strumenti da mettere a disposizione del settore pubblico e di quello privato in tutta Europa;

2. l'ampliamento delle capacità tecnologiche esistenti e la messa in rete dei centri di competenza negli Stati membri, in modo tale che tali capacità rispondano alle esigenze del settore pubblico e dell'industria, anche per quanto riguarda prodotti e servizi che rafforzano la cibersicurezza e la fiducia all'interno del mercato unico digitale;

3. la garanzia di un'ampia mobilitazione di soluzioni di cibersicurezza e fiducia efficaci e all'avanguardia in tutti gli Stati membri. Tale mobilitazione comprende il rafforzamento della sicurezza dei prodotti dalla progettazione alla commercializzazione;

4. il sostegno volto a colmare le lacune di competenze in materia di cibersicurezza, tenendo conto dell'equilibrio di genere, ad esempio, allineando i programmi relativi a tali competenze, adattandoli alle esigenze settoriali specifiche e favorendo l'accesso a corsi di formazione mirati e specializzati;

5. la promozione della solidarietà tra gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala tramite la mobilitazione di servizi di cibersicurezza a livello transfrontaliero, tra cui il sostegno all'assistenza reciproca tra le autorità pubbliche e l'istituzione di una riserva di fornitori di fiducia di servizi di sicurezza gestiti a livello dell'Unione.»;

2) nell'allegato II la sezione «Obiettivo specifico 3 — Cibersicurezza e fiducia» è sostituita dalla seguente:

«Obiettivo specifico 3 — Cibersicurezza e fiducia

3.1. Numero di infrastrutture o strumenti di cibersicurezza, o di entrambi, acquisiti congiuntamente anche nell'ambito del sistema europeo di allerta per la cibersicurezza

3.2. Numero di utenti e comunità di utenti che hanno accesso a strutture di cibersicurezza europee

3.3 Numero di azioni a sostegno della preparazione e della risposta agli incidenti di cibersicurezza nell'ambito del meccanismo per le emergenze di cibersicurezza».

È stata resa una dichiarazione in merito al presente atto, reperibile in GU C, C/2025/308, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/308/oj.