Parlamento europeo
2019-2024

TESTI APPROVATI

P9_TA(2024)0355

Regolamento sulla cibersolidarietà

Risoluzione legislativa del Parlamento europeo del 24 aprile 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2023)0209),

– visti l'articolo 294, paragrafo 2, l'articolo 173, paragrafo 3, e l'articolo 322, paragrafo 1, lettera a), del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C9-0136/2023),

– visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

visto il parere della Corte dei conti del 18 aprile 2023[1],

– visto il parere del Comitato economico e sociale europeo del 13 luglio 2023[2],

visto il parere del Comitato delle regioni del 30 novembre 2023[3],

– visti l'accordo provvisorio approvato dalla commissione competente a norma dell'articolo 74, paragrafo 4, del regolamento e l'impegno assunto dal rappresentante del Consiglio, con lettera del 21 marzo 2024, di approvare la posizione del Parlamento europeo, in conformità dell'articolo 294, paragrafo 4, del trattato sul funzionamento dell'Unione europea,

– visto l'articolo 59 del suo regolamento,

– visti i pareri della commissione per gli affari esteri e della commissione per i trasporti e

---

1 Non ancora pubblicato nella Gazzetta ufficiale.
2 GU L 349 del 29.9.2023, pag. 167.
3 OJ C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

il turismo,

– vista la relazione della commissione per l'industria, la ricerca e l'energia (A9-0426/2023),

1. adotta la posizione in prima lettura figurante in appresso;

2. prende atto della dichiarazione della Commissione allegata alla presente risoluzione, che sarà pubblicata nella *Gazzetta ufficiale dell'Unione europea*, serie C;

3. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

4. incarica la sua Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

P9_TC1-COD(2023)0109

Posizione del Parlamento europeo definita in prima lettura il 24 aprile 2024 in vista dell'adozione del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi *(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],

---

* IL TESTO NON È ANCORA STATO OGGETTO DI REVISIONE GIURIDICO-LINGUISTICA.

1 GU C […] del […], pag. […].

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.***

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***, dato che le pubbliche amministrazioni, le imprese e i cittadini dell'Unione sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero***, e ha introdotto al tempo stesso possibili vulnerabilità***.

(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza ***a livello dell'Unione e su scala mondiale***, compresi gli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che 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 su vasta scala, che possono provocare interruzioni 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 in periodi di tempo molto brevi, 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 digitalizzata 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[5]**.** È necessario accrescere la resilienza dei cittadini, delle imprese, ***comprese le microimprese e le piccole e medie imprese (PMI) nonché le start-up,*** e dei soggetti che gestiscono infrastrutture critiche, tra cui le autorità locali o regionali, contro le crescenti minacce alla cibersicurezza, 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 rilevamento delle minacce e degli incidenti di cibersicurezza 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 su vasta scala ***e di ripresa iniziale dagli stessi***. ***Basandosi sulle strutture esistenti e in stretta cooperazione con le stesse,*** l'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza.

5 https://futureu.europa.eu/it/?locale=it.

(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 di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[6], la raccomandazione (UE) 2017/1584 della Commissione[7], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[8] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[9]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato 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.

---

6 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).

7 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 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).

9 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).

(5) I crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti informatici da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono ***di rafforzare la*** solidarietà ▌ a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi***, come pure la ripresa dai medesimi, in particolare rafforzando le capacità delle strutture esistenti***. Nelle conclusioni del Consiglio su una posizione dell'UE in materia di deterrenza informatica[10] gli Stati membri hanno inoltre invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

(6) La comunicazione congiunta sulla politica di ciberdifesa dell'UE[11], adottata il 10 novembre 2022, ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la realizzazione di un'infrastruttura unionale dei centri operativi di sicurezza ("SOC"), sostenere la costituzione graduale di una forza di 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.

---

10 Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dal Consiglio nella sessione del 23 maggio 2022 (9364/22).

11 Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

(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 su vasta scala ***e gli incidenti equivalenti a incidenti di cibersicurezza su vasta scala, e di rispondere agli stessi***. Di conseguenza si dovrebbe ***istituire*** una ***rete*** paneuropea di ***poli informatici*** (***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***, creare 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 su vasta scala e nella ripresa ***iniziale*** dagli stessi, e istituire un meccanismo di riesame degli incidenti di cibersicurezza per riesaminare e valutare specifici incidenti significativi o 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, da EU-CyCLONe e dal gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555.*** La realizzazione di tali azioni non pregiudica gli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea ("TFUE").

(8) Per conseguire questi obiettivi occorre inoltre modificare il regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio[12] 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 significativi, agli incidenti di cibersicurezza su vasta scala e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala, e ad attenuarne gli effetti.***

---

12 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).

Tali effetti potrebbero 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, nei casi 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 monitorare l'attuazione di questi ultimi.

(9) ***Per rafforzare la risposta dell'Unione alle minacce e agli incidenti di cibersicurezza, è essenziale la cooperazione con le istituzioni internazionali e con i partner internazionali di fiducia e che condividono gli stessi principi. In tale contesto, per partner internazionali di fiducia e che condividono gli stessi principi si dovrebbero intendere i paesi che condividono i principi dell'Unione in materia di democrazia, Stato di diritto, universalità e indivisibilità dei diritti umani e delle libertà fondamentali, 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 del presente regolamento, in particolare il sistema europeo di allerta per la cibersicurezza e la riserva dell'UE per la cibersicurezza. Per quanto riguarda il sistema europeo di allerta per la cibersicurezza e la riserva dell'UE per la cibersicurezza, il regolamento (UE) 2021/694, quale modificato dal presente regolamento, prevede che, se sono soddisfatte determinate condizioni di disponibilità e sicurezza, 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 all'obiettivo specifico 3 del programma Europa digitale. Le condizioni specifiche di partecipazione riguardanti ciascuna azione saranno indicate nei programmi di lavoro pertinenti, in linea con le disposizioni applicabili del 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) 2018/1046 del Parlamento europeo e del Consiglio***[13], 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 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[14].

---

13 ***Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

14 ***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 433I del 22.12.2020, pag. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

(12) ***Benché le misure di prevenzione e preparazione siano essenziali per rafforzare la resilienza dell'Unione nel far fronte a incidenti significativi, 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 di assistenza reciproca, in aggiunta al riporto degli stanziamenti autorizzati ai sensi dell'articolo 12, paragrafo 4, del regolamento finanziario.***

(13) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi ***e la ripresa dai medesimi***, 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 è costituito da 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 strumenti di analisi e di raccolta ***avanzati*** di dati ***pertinenti e, se del caso, anonimizzati***, 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 di cibersicurezza, aumentando il*** rilevamento***, l'aggregazione e l'analisi di dati e informazioni al fine di prevenire le*** minacce e ***gli*** incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche ("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 dell'Unione nel campo della cibersicurezza. Ciò è particolarmente utile nel contesto della condivisione di informazioni 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 a dare attuazione a tali richieste. Se del caso e conformemente al diritto nazionale e dell'Unione, 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 della direttiva (UE) 2022/2555, è fondamentale che si coordini con tale autorità competente per quanto riguarda le richieste di dati e il loro ricevimento.

(15) Nell'ambito del ***sistema*** europeo ***di allerta per la cibersicurezza*** è opportuno istituire diversi ***poli informatici transfrontalieri*** che, a loro volta, dovrebbero riunire i ***poli informatici*** nazionali di almeno tre Stati membri, in modo da sfruttare appieno i vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei ***poli informatici*** transfrontalieri dovrebbe essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce alla cibersicurezza e di favorire l'elaborazione di analisi di alta qualità sulle minacce alla cibersicurezza, in particolare mediante la condivisione di ***informazioni pertinenti e, se del caso, anonimizzate 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. Tali ***poli informatici transfrontalieri*** dovrebbero garantire nuove capacità aggiuntive, basandosi sui SOC e 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 ("ECCC") a seguito di un invito a manifestare interesse al fine di istituire un polo informatico nazionale o di rafforzare le capacità di un polo informatico nazionale esistente dovrebbe acquistare gli strumenti, le infrastrutture e i servizi pertinenti congiuntamente all'ECCC. Tale Stato membro dovrebbe poter beneficiare di una sovvenzione per l'utilizzo degli strumenti, delle infrastrutture e 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 rafforzare le capacità di un polo informatico transfrontaliero esistente, dovrebbe acquistare gli strumenti, le infrastrutture e i servizi pertinenti congiuntamente con l'ECCC. Tale consorzio ospitante dovrebbe poter beneficiare di una sovvenzione per l'utilizzo degli strumenti, delle infrastrutture e dei servizi. La procedura di appalto per l'acquisto degli strumenti, delle infrastrutture e 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.

L'appalto dovrebbe essere conforme all'articolo 165, paragrafo 2, del regolamento (UE) 2018/1046 e all'articolo 90 della decisione n. GB/2023/1 del consiglio di direzione dell'ECCC. I soggetti privati non dovrebbero pertanto essere ammessi a partecipare agli inviti a manifestare interesse per l'acquisto congiunto di strumenti, infrastrutture e servizi con l'ECCC né a ricevere sovvenzioni per l'utilizzo di tali strumenti, infrastrutture e servizi. Tuttavia, gli Stati membri dovrebbero avere la possibilità di 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 nazionale e dell'Unione. Anche i soggetti privati potrebbero 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 rafforzare le capacità di un polo informatico nazionale esistente 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 e 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 volte a rafforzare le capacità del suo polo informatico nazionale di cui al capo II del presente regolamento. 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 europei, 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 nel contesto 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 di quest'ultima. 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 e, se del caso, anonimizzate*** sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati 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 (ad esempio, squadre di pronto intervento informatico ("CERT"), CSIRT, ISAC, operatori di infrastrutture critiche). ***I membri del consorzio ospitante dovrebbero specificare nell'accordo di consorzio le informazioni pertinenti da condividere tra i partecipanti al polo informatico transfrontaliero.*** 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***,*** vulnerabilità ***e quasi incidenti, tecniche e procedure, 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***. I ***poli informatici*** transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri ***poli informatici*** transfrontalieri.

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 emanati dall'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, delle migliori pratiche e dell'attuale funzionamento dei poli informatici transfrontalieri esistenti.

(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 su vasta scala. La direttiva (UE) 2022/2555 istituisce 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 prevede anche l'istituzione di una rete di CSIRT volta a 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 questo 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 ricorda altresì le responsabilità della Commissione nell'ambito del meccanismo unionale di protezione civile ("UCPM") istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, nonché la sua responsabilità per quanto riguarda la fornitura di relazioni analitiche per i dispositivi integrati per la risposta politica alle crisi ("IPCR") ai sensi della decisione di esecuzione (UE) 2018/1993. ***Quando i poli informatici transfrontalieri condividono con EU-CyCLONe*** 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, si ricorda 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 le informazioni di cui al presente considerando siano immediatamente condivise con i rappresentanti degli Stati membri interessati e con la 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, nonché prevedere 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*** di cibersicurezza dovrebbero tenere conto dei lavori ***già realizzati*** in materia di notifica degli incidenti nel contesto dell'attuazione della direttiva (UE) 2022/2555.

(23) Per consentire lo scambio di dati ***e informazioni pertinenti*** sulle minacce alla cibersicurezza 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 e 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 pertanto una forza lavoro qualificata rimane essenziale per una 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 all'organismo 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 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 di riesame degli incidenti 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, il loro scambio a norma del presente regolamento dovrebbe essere limitato alle informazioni pertinenti e commisurate a tale scopo. Tale scambio dovrebbe inoltre tutelare la riservatezza di tali informazioni e proteggere la sicurezza e gli interessi commerciali dei soggetti interessati. La condivisione 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 TLP. Il protocollo TLP (Traffic Light Protocol) 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 lo scambio 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.***

Per quanto riguarda la realizzazione 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 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 nell'attuazione 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, e che le informazioni riservate o classificate ai sensi del diritto nazionale e dell'Unione 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 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 e non incidono sullo scambio di informazioni in altri contesti, ad esempio negli appalti relativi alla riserva.

(28) Alla luce dell'aumento dei rischi e del numero di incidenti informatici 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 e su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta 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.*** Tale strumento 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 di cibersicurezza, 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").

(29) 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 su vasta scala e di ripresa ***iniziale*** dagli stessi, come i servizi forniti dall'Agenzia dell'Unione europea per la cibersicurezza ("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, i gruppi di risposta rapida agli incidenti informatici della PESCO[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***.

[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.

(30) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare ***il meccanismo unionale di protezione civile istituito a norma della decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio[16], i dispositivi integrati dell'UE per la risposta politica alle crisi di cui alla decisione di esecuzione (UE) 2018/1993 del Consiglio[17] (dispositivi IPCR), la raccomandazione 2017/1584 della Commissione[18]*** e la direttiva (UE) 2022/2555. ***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. 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.

---

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 ***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).***

18 ***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).***

(31) 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 una stretta collaborazione e consultazione tra ***gli Stati membri,*** la Commissione***, l'ENISA***, ***e, ove opportuno, l'ECCC***. Nel richiedere un sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza, lo Stato membro dovrebbe fornire informazioni pertinenti che ne giustifichino la necessità.

(32) 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 impiegare 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 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 su vasta scala, al fine di sostenere la ripresa ***iniziale o*** il ripristino ***delle funzionalità essenziali dei servizi forniti dai soggetti operanti in settori ad alta criticità e altri settori critici***.

(33) 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 ai sensi 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 istituito dalla direttiva (UE) 2022/2555 ***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 a livello dell'Unione. I settori o i sottosettori dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("Settori ad alta criticità"). Gli esercizi di verifica coordinata dovrebbero 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 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 (BEREC), le valutazioni coordinate del rischio 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.

---

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.

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

(35) ***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. 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.***

(36) 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 e 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 informatici sui cittadini.

(37) Il meccanismo per le emergenze di cibersicurezza dovrebbe sostenere l'assistenza ***tecnica*** fornita ***da*** uno Stato membro ***a un altro***. Uno Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o 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.

(38) ***Dato il ruolo essenziale svolto dalle imprese private nel rilevamento degli incidenti di cibersicurezza 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 ed equivalenti ad 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 a norma del presente regolamento, anche per quanto riguarda l'affidabilità delle imprese, la loro esperienza e la capacità di gestire informazioni sensibili in modo sicuro.***

(39) ***Al fine di garantire un uso efficace dei finanziamenti dell'Unione, i servizi preimpegnati dovrebbero essere convertiti, 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 e non duplicare le azioni di preparazione che saranno gestite dall'ECCC.***

(40) ***Nell'ambito del meccanismo per le emergenze di cibersicurezza,*** è opportuno istituire gradualmente una riserva per la cibersicurezza a livello dell'Unione, costituita da servizi erogati da fornitori ***di fiducia per sostenere la*** risposta ***e avviare*** azioni di ripresa in caso di incidenti ***di cibersicurezza significativi, su vasta scala ed equivalenti a incidenti su vasta scala che interessano gli Stati membri, le istituzioni, gli organi e le agenzie 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 attuabili 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 altri*** settori critici, a integrazione delle azioni da esse svolte a livello nazionale. ***I servizi di tale riserva possono inoltre 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 incentivando gli investimenti nell'ambito della ricerca e dell'innovazione. È importante tenere conto del quadro europeo in materia di competenze nel settore della cibersicurezza (ECSF) in sede di acquisizione dei servizi per la riserva.*** 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 i potenziali impatti, informazioni sul servizio richiesto a carico della riserva 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) ***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, che è l'ENISA nei casi in cui sia stata incaricata dell'amministrazione e del funzionamento della riserva dell'UE per la cibersicurezza. Le richieste di sostegno da parte di paesi terzi associati al programma Europa digitale dovrebbe essere valutate dalla Commissione. Per facilitare la presentazione e la valutazione delle richieste di sostegno, l'ENISA potrebbe istituire una piattaforma sicura.***

(42) ***Qualora siano ricevute più richieste concomitanti, dovrebbe essere attribuita priorità a tali richieste conformemente ai criteri stabiliti dal presente regolamento. Alla luce degli obiettivi generali del presente regolamento, tali criteri dovrebbero includere la gravità dell'incidente, il tipo di soggetto interessato, il potenziale impatto sugli Stati membri o sugli utenti interessati, la potenziale natura transfrontaliera e il rischio di ricaduta e le misure già adottate dall'utente per assistere la risposta e la ripresa iniziale. Alla luce degli stessi obiettivi e dato che le richieste degli utenti degli Stati membri sono intese esclusivamente a sostenere soggetti in tutta l'Unione che operano in settori ad alta criticità o in altri settori critici, è opportuno attribuire maggiore priorità alle richieste degli utenti degli Stati membri qualora due o più richieste sono considerati 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.***

(43) ***La Commissione dovrebbe avere la responsabilità generale del funzionamento 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 effettuato conformemente alle norme applicabili a norma del regolamento (UE) 2018/1046 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.***

(44) ***Gli Stati membri dovrebbero svolgere un ruolo chiave nella costituzione, nella diffusione e nella fase successiva alla realizzazione 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 pertinenti programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694. A norma dell'articolo 24, paragrafo 6, del regolamento (UE) 2021/694, tali programmi di lavoro dovrebbero essere adottati dalla Commissione mediante atti di esecuzione secondo la procedura d'esame di cui all'articolo 5 del regolamento (UE) n. 182/2011. 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.***

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

(46) 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 minimi da includere nel corrispondente bando di gara, in modo da garantire che siano soddisfatte le esigenze delle autorità e dei soggetti degli Stati membri che operano in settori ***ad alta criticità o 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 aggiuntivi rispetto a quelli stabiliti nel presente regolamento. È importante incoraggiare la partecipazione dei fornitori più piccoli, attivi a livello regionale e locale.***

(47) ***Nel selezionare i fornitori da includere nella riserva, l'amministrazione aggiudicatrice dovrebbe mirare a garantire che la riserva, 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 abbiano requisiti linguistici specifici, in modo che i servizi di sostegno della riserva possano essere forniti in una lingua tra le lingue ufficiali dell'Unione o dello Stato membro, che potrebbe 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 e i servizi siano stati acquistati in tali lingue per tale utente, l'utente dovrebbe poter specificare, nella richiesta di sostegno della riserva, in quali di tali lingue dovrebbero essere forniti i servizi in relazione all'incidente specifico che ha dato origine alla richiesta.***

(48) 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*** ai sensi del regolamento (UE) 2019/881 per i servizi di sicurezza gestiti nei settori che rientrano nel meccanismo per le emergenze di cibersicurezza.

(49) 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 su vasta scala, ***la Commissione o*** EU-CyCLONe***, con il consenso dello Stato membro interessato,*** dovrebbero essere in grado di chiedere all'ENISA di riesaminare e valutare le minacce, le vulnerabilità ***sfruttabili note*** e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Dopo il 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, ▌della Commissione e di altre istituzioni, organi e organismi dell'UE 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, gli impatti 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 come disposto dal presente regolamento. La relazione dovrebbe essere presentata a EU-CyCLONe, alla rete di CSIRT e alla Commissione ***e dovrebbe*** essere integrata nelle ***loro*** attività ***e in quelle dell'ENISA***. Se l'incidente riguarda un paese terzo ***associato al programma Europa digitale***, la Commissione ***dovrebbe condividere*** inoltre la relazione con l'alto rappresentante.

(50) Tenendo conto della natura imprevedibile degli attacchi di cibersicurezza 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 su vasta scala contribuisce alla protezione dell'Unione nel suo complesso***, e in particolare del suo mercato interno e della sua industria***. ***Tali attività potrebbero contribuire ulteriormente alla diplomazia informatica dell'UE.*** I paesi terzi associati al programma Europa digitale possono quindi essere sostenuti dalla 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 su vasta scala.

(51) ***Le condizioni stabilite per la riserva dell'UE per la cibersicurezza e per i fornitori di fiducia 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 il servizio 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 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, il paese terzo avrebbe dovuto adottare misure adeguate per prepararsi a incidenti di cibersicurezza significativi o equivalenti a incidenti su vasta scala. In terzo luogo, il sostegno fornito dalla riserva 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 questo terzo criterio, la Commissione dovrebbe consultare l'alto rappresentante per allineare la concessione di tale sostegno alla politica estera e di sicurezza comune.***

(52) ***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 difesa e sicurezza 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 vale per i rinnovi e per le proposte ordinarie di modifica o revoca di tali atti. Qualora, in via eccezionale, il Consiglio ritenga che vi sia stato un cambiamento significativo delle circostanze in relazione al terzo criterio, esso dovrebbe poter agire di propria iniziativa e 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 a tali richieste e s 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 realizzati.***

(53) 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.

(54) ***La comunicazione della Commissione sull'Accademia per le competenze in materia di cibersicurezza, pubblicata il 18 aprile 2023, ha riconosciuto la carenza di professionisti qualificati. Tali figure sono necessarie per perseguire gli obiettivi del presente regolamento. L'UE ha urgentemente bisogno di professionisti dotati di capacità e competenze per prevenire, individuare e scoraggiare gli attacchi informatici e difendere l'UE, 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, compresi il settore privato, il mondo accademico e il 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 e per evitare che il divario di competenze non aumenti maggiormente in alcune regioni rispetto ad 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 (R&I) nel settore della cibersicurezza. Ciò contribuisce 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 il settore privato, la società civile e il mondo accademico.

(56) Il presente regolamento dovrebbe tener conto dell'impegno della dichiarazione europea sui diritti e i principi digitali per il decennio digitale per proteggere gli interessi delle nostre democrazie, dei nostri cittadini, delle nostre imprese e delle nostre istituzioni pubbliche 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]***.

---

20 ***Accordo interistituzionale "Legiferare meglio" tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea (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).***

(59) La Commissione dovrebbe effettuare periodicamente una valutazione delle misure di cui al presente regolamento. La prima valutazione dovrebbe aver luogo nei primi due anni dalla data di applicazione del presente regolamento e successivamente almeno ogni quattro anni, tenendo conto del calendario della revisione del quadro finanziario pluriennale. 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.

(60) L'obiettivo del presente regolamento può essere conseguito meglio a livello di Unione piuttosto che dagli Stati membri. L'Unione può quindi intervenire in base ai principi di sussidiarietà e proporzionalità sanciti dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per il conseguimento di tale obiettivo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I

OBIETTIVI GENERALI, OGGETTO E DEFINIZIONI

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 di cibersicurezza, e di preparazione e risposta agli stessi, in particolare mediante:

(a) ***l'istituzione*** di una ***rete*** paneuropea di ***poli informatici*** ("***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) la creazione di un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri ***e altri utenti*** nella preparazione e nella risposta agli incidenti di cibersicurezza significativi***,*** su vasta scala ***ed equivalenti a incidenti su vasta-scala, nella mitigazione del loro impatto*** e nella ripresa immediata dagli stessi;

(c) l'istituzione di un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di incidenti significativi o 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***.

2 bis. ***Il conseguimento degli obiettivi generali è perseguito mediante gli obiettivi specifici seguenti:***

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

(b) rafforzare la preparazione dei soggetti che operano in settori ***ad alta criticità e 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*** gli incidenti di cibersicurezza significativi***,*** su vasta scala ***o equivalenti ad 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, riesaminando e valutando gli incidenti significativi o su vasta scala, traendone anche insegnamenti e, se del caso, formulando raccomandazioni.

▌

2 ter. ***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, dal gruppo di cooperazione NIS e da EU-CyCLONe.***

3. 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.***

4. ***Lo scambio di informazioni riservate ai sensi della normativa dell'Unione o nazionale è limitato a quanto pertinente e proporzionato allo scopo di tale scambio. Lo scambio di tali informazioni a norma del presente regolamento tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali dei soggetti interessati. Ciò non comporta 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 e, 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 ***e 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 o in altri settori*** critici": il tipo di soggetti elencati negli allegati I e II della direttiva (UE) 2022/2555;

(6) "gestione degli incidenti": la gestione degli incidenti quale definita all'articolo 6, punto 8), della 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 di cibersicurezza che soddisfa i criteri stabiliti all'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555;

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

(12) "incidente di cibersicurezza equivalente a incidente su larga scala": nel caso delle istituzioni, degli organi e degli organismi dell'Unione, un incidente grave quale definito all'articolo 3, punto (8), del regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio[22] 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;

(13) "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;

---

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).***

(14) "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 12, paragrafo 6, del presente regolamento, l'ENISA;

▌

(15) "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;

(16) "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 16 del presente regolamento.

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 e risposta alle minacce informatiche 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 della direttiva (UE) 2022/2555, cooperando con essi e rafforzandone le capacità;

(a) 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***;

(b) ***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 e 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 ("polo informatico nazionale")***.

▌

1 ter. ***Nell'ambito delle funzioni di cui al paragrafo 1 bis, 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. Se del caso e conformemente al diritto nazionale e dell'Unione, le informazioni richieste o ricevute dai poli informatici nazionali possono includere dati raccolti mediante telemetria, sensori e registrazioni.***

1 quater. ***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 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 di cibersicurezza e per contribuire a un polo informatico transfrontaliero di cui all'articolo 5 del presente regolamento; e***

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

▌

3. ***Uno Stato membro*** selezionato ai sensi ***dell'articolo 8 bis,*** 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 ("consorzio ospitante")***.

1 bis. ***Un consorzio ospitante è un consorzio composto da almeno tre Stati membri partecipanti che hanno concordato di stabilire e sostenere l'acquisizione di strumenti, infrastrutture e servizi per un polo informatico transfrontaliero di cui al paragrafo 3 bis e il suo funzionamento;***

3. ***Se un*** consorzio ospitante ***è selezionato a norma dell'articolo 8 bis, 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 8 bis, 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.

3 bis. 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 e, 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.

4. 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 del polo informatico transfrontaliero al presente regolamento e alla*** convezione di accoglienza e di utilizzo ***è determinata nell'accordo di consorzio scritto di cui al paragrafo 3***.

5. 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 e 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 scambino tra loro, conformemente all'accordo di consorzio di cui all'articolo 5, paragrafo 3***, informazioni pertinenti ***e, se del caso, anonimizzate 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 o fasi di risposta e ripresa, oppure 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 le informazioni*** di cui al paragrafo 1 e le condizioni di scambio di tali informazioni***. L'accordo può specificare che le informazioni sono scambiate in conformità del diritto dell'Unione e nazionale***;

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

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

2 bis. 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 conclusi.

3. Lo scambio di 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, senza indebito ritardo e al più tardi 12 mesi dopo la data di entrata in vigore del presente regolamento, l'ENISA, in stretta consultazione con la Commissione, 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 degli accordi di cooperazione per i 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 1, i tipi di informazioni da condividere.

1. 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 ***delle informazioni e*** dei dati scambiati 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, del presente regolamento*** 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 8 bis

Finanziamento del sistema europeo di allerta per la cibersicurezza

1. A seguito di un invito a manifestare interesse, gli Stati membri che intendono partecipare al sistema europeo di allerta per la cibersicurezza sono selezionati dal Centro europeo di competenza per la cibersicurezza ("ECCC") per partecipare con quest'ultimo a un appalto congiunto di strumenti, infrastrutture e servizi, al fine di istituire poli informatici nazionali di cui all'articolo 4, paragrafo 1, o di rafforzare le capacità di quelli esistenti. L'ECCC può attribuire sovvenzioni agli Stati membri selezionati per finanziare il funzionamento di tali strumenti, infrastrutture e servizi. Il contributo finanziario dell'Unione copre fino al 50 % dei costi di acquisizione di strumenti, infrastrutture e servizi e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dallo Stato membro. Prima di avviare la procedura di acquisizione di strumenti, infrastrutture e servizi, l'ECCC e lo Stato membro concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti, delle infrastrutture e dei servizi.

2. *Se un polo informatico nazionale di uno Stato membro non partecipa a un polo informatico transfrontaliero entro due anni dalla data di acquisizione degli strumenti, delle infrastrutture e 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 avrà 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 e servizi. L'ECCC può attribuire al consorzio ospitante una sovvenzione per finanziare il funzionamento degli strumenti, delle infrastrutture e dei servizi. Il contributo finanziario dell'Unione copre fino al 75 % dei costi di acquisizione degli strumenti, delle infrastrutture e dei servizi e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dal consorzio ospitante. Prima di avviare la procedura di acquisizione di strumenti, infrastrutture e servizi, l'ECCC e il consorzio ospitante concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti, delle infrastrutture e dei servizi.*

4. ***L'ECCC prepara, almeno ogni due anni, una mappatura degli strumenti, delle infrastrutture e dei servizi necessari e di qualità adeguata per istituire o rafforzare i poli informatici nazionali e transfrontalieri, 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 9

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, prepararsi all'impatto a breve termine degli incidenti di cibersicurezza significativi ▌ su vasta scala ***ed equivalenti a incidenti su vasta scala*** nonché attenuare tale impatto (il "meccanismo").

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

2. 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 e in particolare dell'obiettivo specifico 3.

2 bis. ***Le azioni nell'ambito del meccanismo per le emergenze di cibersicurezza sono attuate principalmente mediante l'ECCC in conformità del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, fatta eccezione per le azioni di attuazione della riserva dell'UE per la cibersicurezza di cui all'articolo 10, paragrafo 1, lettera b), che sono attuate dalla Commissione e dall'ENISA.***

Articolo 1

Tipi di azioni

1. 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 11;

ii) altre azioni di preparazione per i soggetti che operano in settori altamente critici e in altri settori critici, come specificato all'articolo 11 bis;

b) azioni ▌ a sostegno della risposta agli incidenti di cibersicurezza significativi***,*** su vasta scala ***ed equivalenti a incidenti di cibersicurezza su vasta scala*** e ***che avviano la*** ripresa ▌ dagli stessi, che devono essere condotte da fornitori di fiducia ***di servizi di sicurezza gestiti*** che partecipano alla riserva dell'UE per la cibersicurezza istituita ai sensi dell'articolo 12;

c) azioni di assistenza reciproca ***di cui all'***articolo ***16 bis***.

Articolo 11

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.

-1 bis. La verifica coordinata della preparazione può consistere in attività di preparazione, quali i test di penetrazione e la valutazione delle minacce.

-1 ter. Il sostegno alle azioni di preparazione di cui al presente articolo è fornito agli Stati membri principalmente sotto forma di sovvenzioni e alle condizioni definite nei pertinenti programmi di lavoro di cui all'articolo 24 del programma Europa digitale.

1. Al fine di sostenere la verifica coordinata della preparazione dei soggetti di cui all'articolo 10, paragrafo 1, lettera a), ***punto i),*** 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 di cui 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 avviene su base volontaria***.

1 bis. ***Nell'individuare i settori o sottosettori di cui al paragrafo 1, la Commissione tiene conto delle valutazioni coordinate del rischio e dei test di resilienza a livello di Unione nonché e dei relativi risultati.***

2. Il gruppo di cooperazione NIS, in collaborazione con la Commissione, ***l'alto rappresentante e*** l'ENISA e***, nell'ambito del suo mandato, EU-CyCLONe***, elabora scenari di rischio e metodologie comuni per gli esercizi di verifica coordinata ***a norma dell'articolo 10, paragrafo 1, lettera a), punto i), del presente regolamento e, se del caso, per altre azioni di preparazione a norma dell'articolo 10, paragrafo 1, lettera a), punto ii)***.

3. ***Quando un soggetto che opera in un settore ad alta criticità partecipa volontariamente a esercizi di verifica coordinata e tali esercizi danno luogo a raccomandazioni di misure specifiche, che possono essere integrate dal soggetto partecipante in un piano di ripristino, l'autorità dello Stato membro responsabile dell'esercizio di verifica riesamina, se del caso, il seguito dato a tali misure dai soggetti partecipanti al fine di rafforzare la preparazione.***

Articolo 11 bis

Altre azioni di preparazione

1. *Il meccanismo per le emergenze di cibersicurezza sostiene inoltre le azioni di preparazione non contemplate dall'articolo 11 del presente regolamento in relazione alle azioni coordinate di preparazione dei soggetti. Tali azioni comprendono azioni di preparazione per i soggetti in settori non individuati per la verifica coordinata a norma dell'articolo 11. 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 definite nei pertinenti programmi di lavoro di cui all'articolo 24 del regolamento (UE) 2021/694.*

Articolo 12

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***,*** su vasta scala***, o equivalenti a quelli 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 selezionati in base ai criteri di cui all'articolo 16. La riserva ***può includere*** servizi preimpegnati. I servizi ***preimpegnati di un prestatore di fiducia sono convertibili, nei casi in cui tali servizi non siano utilizzati per la risposta agli incidenti durante il periodo per il quale tali servizi sono preimpegnati, in servizi di preparazione relativi alla prevenzione e alla risposta agli incidenti. La riserva è realizzabile 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 17, paragrafo 1***.

3. Gli utenti che usufruiscono dei servizi della 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-EU, 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 17, paragrafo 3.

5. 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 collaborazione con il gruppo di coordinamento 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 riviste ogni due anni. La Commissione informa il Parlamento europeo e il Consiglio in merito a tali priorità e alla loro revisione.***

6. ***Fatta salva la responsabilità generale della*** Commissione ***per l'attuazione della riserva dell'UE per la cibersicurezza di cui al paragrafo 5 e fatto salvo un accordo di contributo quale definito all'articolo 2, punto (18), del regolamento finanziario, 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.***

7. ***L'ENISA prepara, almeno ogni due anni, una mappatura dei servizi necessari agli utenti di cui al paragrafo 3, lettere a) e b). 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. 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 e*** 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)***.

8. ***Alla*** Commissione ***è conferito il potere di adottare*** atti ***delegati conformemente all'articolo 20 bis 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 7 e può scambiare pareri e cooperare con il gruppo di cooperazione NIS e l'ENISA.***

Articolo 13

Richieste di sostegno della riserva dell'UE per la cibersicurezza

1. Gli utenti di cui all'articolo 12, paragrafo 3, possono richiedere servizi della riserva dell'UE per la cibersicurezza a sostegno della risposta agli incidenti di cibersicurezza significativi**,** su vasta scala ***o equivalenti a incidenti di cibersicurezza 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 12, 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 nel modo seguente:***

a) nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera a), del presente regolamento, tali richieste sono trasmesse tramite il punto di contatto unico designato o istituito dallo Stato membro in conformità dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555;

b) nel caso dell'utente di cui all'articolo 12, paragrafo 3, lettera b), del presente regolamento, tali richieste sono trasmesse dal CERT-UE;

c) nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera c), del presente regolamento, tali richieste sono trasmesse tramite il punto di contatto unico di cui all'articolo 17, paragrafo 4, del presente regolamento.

4. ***In caso di richieste da parte degli utenti di cui all'articolo 12, paragrafo 3, lettera a), del presente regolamento,*** 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) lo Stato membro o gli Stati membri e gli utenti interessati, compreso il rischio di propagazione a un altro Stato membro, nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera a), del presente regolamento;

      ii) le istituzioni, gli organi e gli organismi dell'Unione interessati, nel caso dell'utente di cui all'articolo 12, paragrafo 3, lettera b), del presente regolamento;

      iii) i paesi associati al programma Europa digitale interessati, nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera c), del presente regolamento;

a bis) informazioni sul servizio richiesto, tra cui l'uso previsto del sostegno richiesto, compresa un'indicazione delle esigenze stimate;

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

c) ***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, mediante atti di esecuzione, specificare ulteriormente le modalità ***procedurali*** dettagliate ***per il modo in cui i*** servizi di sostegno della riserva dell'UE per la cibersicurezza ***sono richiesti ed è data una risposta a norma del presente articolo, dell'articolo 14, paragrafo 1, e dell'articolo 17, paragrafo 4 bis, quali le modalità di presentazione delle richieste e di trasmissione delle risposte e dei modelli per le relazioni di cui all'articolo 14, paragrafo 6***. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.

Articolo 14

Attuazione del sostegno della riserva dell'UE per la cibersicurezza

1. ***Nel caso di richieste degli utenti di cui all'articolo 12, 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 12, paragrafo 3, lettere a) e b), senza indugio e in ogni caso entro 48 ore dalla presentazione della richiesta per garantire l'efficacia dell'azione di sostegno. L'amministrazione aggiudicatrice informa il Consiglio e la Commissione dei risultati della procedura.***

1 bis. ***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 nazionale e dell'Unione 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.***

2. ***Nel valutare le singole*** richieste ***ai sensi dell'articolo 14, paragrafo 1 e dell'articolo 17, paragrafo 4 bis, l'amministrazione aggiudicatrice o la Commissione, a seconda dei casi, valuta innanzitutto se i criteri di cui all'articolo 13, paragrafi 1, e 2, sono soddisfatti. In tal caso, essi valutano l'adeguatezza della durata e della natura del sostegno tenendo conto dell'obiettivo di cui all'articolo 1, paragrafo 2, lettera b), e, se del caso, dei seguenti criteri:***

a) la ***portata e la*** gravità dell'incidente di cibersicurezza;

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

c) l'impatto potenziale sugli Stati membri***, sulle istituzioni, sugli organi e 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 13, paragrafo 2, e all'articolo 13, paragrafo 5, lettera b).

2 bis. Per definire l'ordine di priorità delle richieste, in caso di richieste concomitanti da parte degli utenti di cui all'articolo 12, paragrafo 3, si tiene conto, se del caso, dei criteri di cui al paragrafo 2, fatto salvo il principio di leale cooperazione tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione, e qualora due o più richieste siano considerate equivalenti in base ai criteri di cui al paragrafo 2 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 12, paragrafo 6, del presente regolamento, l'ENISA e la Commissione cooperano strettamente per dare priorità alle richieste in linea con il presente paragrafo.

3. I servizi della riserva dell'UE per la cibersicurezza sono forniti in conformità di accordi specifici stipulati tra il fornitore di ***fiducia*** 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, l'utente e l'entità interessata. Tutti gli accordi di cui al presente paragrafo*** includono***, tra l'altro,*** condizioni di responsabilità.

4. Gli accordi di cui al paragrafo 3 ***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***.

5. La Commissione***,*** l'ENISA ***e gli utenti della riserva*** 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.

5 bis. Gli utenti possono utilizzare i servizi della riserva dell'UE per la cibersicurezza forniti in risposta a una richiesta a norma dell'articolo 13, paragrafo 1, del presente regolamento solo per sostenere la risposta agli incidenti 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 altri settori critici, nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera a), e soggetti equivalenti nel caso degli utenti di cui all'articolo 12, paragrafo 3, lettera c); e

b) le istituzioni, gli organi e gli organismi dell'Unione, nel caso dell'utente di cui all'articolo 12, paragrafo 3, lettera b).

6. Entro ***due mesi*** dalla fine ***di un***'azione di sostegno, ***qualsiasi utente che ha ricevuto sostegno fornisce*** una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti***, nel modo seguente:***

a) gli utenti di cui all'articolo 12, paragrafo 3, lettera a), del presente regolamento trasmettono la relazione di sintesi alla Commissione, all'ENISA, alla rete di CSIRT e a EU-CyCLONe;

b) l'utente di cui all'articolo 12, paragrafo 3, lettera b), del presente regolamento trasmette la relazione di sintesi alla Commissione, all'ENISA e all'IICB;

c) gli utenti di cui all'articolo 12, paragrafo 3, lettera c), del presente regolamento condividono tale relazione con la Commissione, che la condividerà con il Consiglio e l'alto rappresentante.

6 bis. ***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 12, paragrafo 6, 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 12, paragrafo 3, lettera c), e, se necessario ai fini della definizione delle priorità a norma del presente articolo, le richieste ricevute dagli utenti di cui all'articolo 12, paragrafo 3, lettera a) o b). Gli obblighi di cui al presente paragrafo lasciano impregiudicato l'articolo 14 del regolamento (UE) 2019/881.***

7. ***Nel caso degli utenti di cui all'articolo 12, 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.

7 bis. ***Nel caso degli utenti di cui all'articolo 12, 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.***

I

Articolo 16

Fornitori di fiducia

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) 2018/1046 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*** includa servizi che possano essere realizzabili 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'UE, 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'UE.

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 di selezione 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/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 realizzazione 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) .../... del Parlamento europeo e del Consiglio***[23] ***(2022/0272 (COD))***;

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

---

23 ***Regolamento (UE) .../... del Parlamento europeo e del Consiglio, del …, relativo a ... (GU L, …, ELI: …).***

h) il fornitore è in grado di prestare il servizio in tempi brevi nello Stato membro o 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 dell'Unione o di uno Stato membro come richiesto, se del caso, dallo*** Stato membro o ***dagli*** Stati membri ***o dagli utenti di cui all'articolo 12, paragrafo 3, lettere b) e c),*** 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 un termine di due anni dalla data di applicazione del sistema***;

▌

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.

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

Articolo 16 bis

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 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 è concesso sotto forma di sovvenzioni e alle condizioni definite nei pertinenti programmi di lavoro di cui all'articolo 24 del programma Europa digitale.*

Articolo 17

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***. ***Tali accordi includono disposizioni che impongono al paese terzo associato al programma Europa digitale di rispettare gli obblighi di cui ai paragrafi 1 bis e 4 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.***

1 bis. ***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, i paesi terzi ***associati al programma Europa digitale*** forniscono alla Commissione ▌ informazioni sulle loro 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***,*** su vasta scala ***o equivalenti a quelli su vasta scala,*** nonché informazioni sui soggetti nazionali responsabili, compresi i CSIRT 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 condivide tali informazioni con l'alto rappresentante e l'ENISA al fine di agevolare la consultazione di cui al paragrafo 6.***

1 ter. 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 equivalenti a quelli su vasta scala, sulla base delle informazioni di cui al paragrafo 1 bis; 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 tale valutazione, la Commissione consulta l'alto rappresentante per quanto riguarda il criterio di cui alla lettera c) del presente paragrafo.

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 1 quater per autorizzare la fornitura di sostegno a titolo della riserva dell'UE per la cibersicurezza nei confronti di tale paese.

1 quater. Il Consiglio può adottare gli atti di esecuzione di cui al paragrafo 1 ter. Tali atti di esecuzione si applicano al massimo per un anno e sono rinnovabili. Gli atti di esecuzione 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. Il Consiglio adotta gli atti di esecuzione di cui al presente paragrafo, di norma, entro otto settimane dall'adozione della proposta della Commissione.

1 quinquies. Il Consiglio può modificare o abrogare gli atti di esecuzione di cui al paragrafo 1 ter 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 1 ter, lettera c), il Consiglio può modificare o abrogare l'atto di esecuzione di cui al paragrafo 1 ter su iniziativa debitamente motivata di uno o più Stati membri.

1 sexies. Nell'esercizio delle sue competenze di esecuzione a norma del presente articolo, il Consiglio applica il paragrafo 1 ter e spiega la sua valutazione di tali criteri. In particolare, quando agisce di propria iniziativa a norma del paragrafo 1 quinquies, secondo comma, il Consiglio illustra il cambiamento significativo di cui a tale comma.

2. 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.

3. 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*** e le autorità di gestione delle crisi informatiche.

4. 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.

4 bis. ***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, conformemente al paragrafo 1 ter. Una risposta è trasmessa senza indebito ritardo agli utenti di cui all'articolo 12, paragrafo 3, lettera c).***

6. ***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 17 bis

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 quelli 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 quelli su vasta scala che comporti il ricorso ai dispositivi integrati dell'UE per la risposta politica alle crisi (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 procedure pertinenti nell'ambito dei dispositivi IPCR.*

Capo IV

MECCANISMO DI RIESAME DEGLI INCIDENTI DI CIBERSICUREZZA

Articolo 18

Meccanismo 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, le vulnerabilità ***sfruttabili note*** e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Al termine del riesame e della valutazione di un incidente, l'ENISA presenta una relazione di riesame dell'incidente ***volta a trarre gli opportuni insegnamenti per evitare o attenuare futuri incidenti a EU-CyCLONe,*** alla rete di CSIRT, ***agli Stati membri interessati*** e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare alla luce di quelli stabiliti negli articoli 15 e 16 della direttiva (UE) 2022/2555. ***Quando un incidente ha un impatto su un paese terzo associato al programma Europa digitale, l'ENISA condivide la relazione anche con il Consiglio. In tali casi***, la Commissione condivide la relazione con l'alto rappresentante.

2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, ***dell'industria, inclusi i*** fornitori di servizi di sicurezza gestiti***,*** e degli 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 a norma della direttiva (UE) 2022/2555 degli Stati membri interessati, collabora anche con i soggetti interessati da incidenti di cibersicurezza significativi o su vasta scala***. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.

3. La relazione comprende un riesame e un'analisi dello specifico incidente di cibersicurezza significativo o 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 nazionale o dell'Unione in materia di protezione delle informazioni sensibili o classificate. ***Se richiesto da uno o più Stati membri interessati o altri utenti di cui all'articolo 12, paragrafo 3, la relazione contiene solo dati anonimizzati. Essa non include dettagli sulle vulnerabilità sfruttate attivamente che rimangono non risolte.***

4. Ove opportuno, la relazione 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. Tale ***relazione*** contiene solo informazioni pubbliche ***affidabili o altre informazioni per cui è stato ottenuto il consenso dello Stato membro o degli Stati membri interessati e, per quanto riguarda le informazioni relative a un utente di cui all'articolo 12, paragrafo 3, lettere b) o c), il consenso di tale utente***.

Capo V

DISPOSIZIONI FINALI

Articolo 19

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:

(1) è inserita la seguente lettera a bis):

"a bis) sostenere lo sviluppo di un ***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;";

(2) è aggiunta la seguente lettera g):

"g) istituire e gestire un meccanismo per le emergenze di cibersicurezza inteso a sostenere gli Stati membri nella preparazione agli incidenti di cibersicurezza significativi e nella risposta agli stessi, a integrazione delle risorse e delle capacità nazionali e di altre forme di sostegno disponibili a livello di Unione, compresa l'istituzione di una riserva dell'UE per la cibersicurezza.";

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, fatta eccezione per le azioni di attuazione della riserva dell'UE per la cibersicurezza, che sono attuate dalla Commissione e***, in conformità dell'articolo 12, paragrafo 6, del regolamento (UE) .../... [inserire il riferimento al regolamento sulla cibersolidarietà],*** dall'ENISA.";

(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:

"8. In deroga all'articolo 12, paragrafo ***1***, del regolamento (UE, Euratom) 2018/1046, 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 di assistenza reciproca*** 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 (UE, Euratom) 2018/1046.***";

(3) l'articolo 12 è così modificato:

(1) il paragrafo 5 è sostituito dal seguente:

"5. 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 non siano ammessi a partecipare a tutte o ad alcune delle azioni nell'ambito dell'obiettivo specifico 3 per ragioni di sicurezza debitamente giustificate. In tali casi, gli inviti a presentare proposte e i bandi d'appalto sono rivolti esclusivamente ai soggetti giuridici stabiliti o considerati stabiliti negli Stati membri e controllati da Stati membri o da cittadini di Stati membri.

Il primo comma del presente paragrafo 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 a tale azione:

a) esiste un rischio reale, alla luce dei risultati della mappatura di cui all'articolo 8 bis, paragrafo 4, del regolamento (UE) .../... [regolamento sulla cibersolidarietà], che gli strumenti, le infrastrutture e 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; e

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.

Il primo comma del presente paragrafo non si applica, per quanto riguarda i soggetti giuridici stabiliti nell'Unione ma controllati da paesi terzi, alle azioni di attuazione della riserva dell'UE per la cibersicurezza se entrambe le condizioni seguenti sono soddisfatte:

a) esiste un rischio reale, alla luce dei risultati della mappatura di cui all'articolo 12, paragrafo 7, del regolamento (UE) .../... [regolamento sulla cibersolidarietà], 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; e

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.";

(2) 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 del presente paragrafo 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, secondo comma, del presente articolo; e

b) volte ad attuare la riserva dell'UE per la cibersicurezza nei casi in cui si applica il paragrafo 5, terzo comma, del presente articolo.";

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

"2. Il Programma può concedere finanziamenti in tutte le forme previste dal regolamento ***(UE, Euratom) 2018/1046***, 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[27] e 2014/25/UE[28] 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 istituita dall'articolo 12 del regolamento (UE) ***.../... [regolamento sulla cibersolidarietà]***, 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 linea con l'articolo 10. 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) **.../...** [rifusione del RF], 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 istituita dall'articolo 12 del regolamento (UE) ***.../... [regolamento sulla cibersolidarietà]***, 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 e 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 e gli organismi dell'Unione. In deroga all'articolo 169, paragrafo 3, del regolamento (UE) **.../...** [rifusione del RF], la 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.";

(4) è aggiunto l'articolo 16 bis seguente:

"***Articolo 16 bis***

Nel caso di azioni volte ad attuare il ***sistema*** europeo ***di allerta per la cibersicurezza*** stabilito dall'articolo 3 del regolamento (UE) ***.../... [regolamento sulla cibersolidarietà]***, le norme applicabili sono quelle sancite agli articoli 4 e 5 del regolamento (UE) ***.../... [regolamento sulla cibersolidarietà]***. In caso di contrasto tra le disposizioni del presente regolamento e gli articoli 4 e 5 del regolamento (UE) ***.../... [regolamento sulla cibersolidarietà]***, prevalgono questi ultimi e si applicano a tali azioni specifiche.

Nel caso della riserva dell'UE per la cibersicurezza istituita dall'articolo 12 del regolamento (UE) .../... [regolamento sulla cibersolidarietà], norme specifiche per la partecipazione di paesi terzi associati al programma sono stabilite all'articolo 17 del regolamento (UE) .../... [regolamento sulla cibersolidarietà]. In caso di contrasto tra le disposizioni del presente regolamento e l'articolo 17 del regolamento (UE) .../... [regolamento sulla cibersolidarietà], prevale quest'ultimo e si applica a tali azioni specifiche.";

(5) l'articolo 19 è sostituito dal seguente:

"Le sovvenzioni nell'ambito del Programma sono attribuite e gestite conformemente al titolo VIII del regolamento ***(UE, Euratom) 2018/1046*** e possono coprire fino al 100 % dei costi ammissibili, fatto salvo il principio di cofinanziamento stabilito all'articolo 190 del regolamento ***(UE, Euratom) 2018/1046***. 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*** di cui all'articolo 4 del regolamento ***(UE) .../... [regolamento sulla cibersolidarietà]*** e al consorzio ospitante di cui all'articolo 5 del regolamento ***(UE) .../... [regolamento sulla cibersolidarietà]***, in conformità dell'articolo 195, primo comma, lettera d), del regolamento ***(UE, Euratom) 2018/1046***.

Il sostegno erogato sotto forma di sovvenzioni per il meccanismo per le emergenze di cibersicurezza di cui all'articolo ***9*** del regolamento ***(UE) .../... [regolamento sulla cibersolidarietà]*** 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 ***(UE, Euratom) 2018/1046***.

Per le azioni specificate nell'articolo 10, paragrafo 1, lettera c), del regolamento ***(UE) .../... [regolamento sulla cibersolidarietà]***, l'ECCC informa la Commissione e l'ENISA sulle richieste di sovvenzioni dirette degli Stati membri senza invito a presentare proposte.

A sostegno dell'assistenza reciproca per la risposta a un incidente di cibersicurezza significativo o su vasta scala, come definito all'articolo 10, lettera c), del regolamento ***(UE) .../... [regolamento sulla cibersolidarietà]***, e in conformità dell'articolo 193, paragrafo 2, secondo comma, lettera a), del regolamento ***(UE, Euratom) 2018/1046***, in casi debitamente giustificati i costi possono essere considerati ammissibili anche se sono stati sostenuti prima della presentazione della domanda di sovvenzione.";

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

Articolo 20

Valutazione ***e riesame***

1. Entro [***due*** anni dalla data di applicazione del presente regolamento] ***e successivamente almeno ogni quattro anni***, la Commissione ***effettua una valutazione del funzionamento delle misure stabilite nel 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 le infrastrutture, gli strumenti e 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;***

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

c) l'uso e l'efficacia della riserva dell'UE per la cibersicurezza in relazione al tipo 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, 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 20 bis

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 12, paragrafo 8, è conferito alla Commissione per un periodo di cinque anni a decorrere da ... [data di entrata in vigore dell'atto legislativo di base]. 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 12, paragrafo 8, 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 12, paragrafo 8, 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 21

Procedura di comitato

1. La Commissione è assistita dal comitato di coordinamento del programma Europa digitale istituito dal 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 22

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 …, il

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*

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 implementazione di soluzioni di cibersicurezza e fiducia efficaci e all'avanguardia in tutti gli Stati membri. Tale implementazione 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 tramite l'introduzione 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 cibersicurezza di fiducia 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".

I

ALLEGATO ALLA RISOLUZIONE LEGISLATIVA

Dichiarazione della Commissione relativa al bilancio in riferimento al regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi

(*Regolamento sulla cibersolidarietà*))*

1. La scheda finanziaria legislativa della Commissione che accompagna la proposta di regolamento sulla cibersolidarietà è stata pubblicata nell'aprile 2023. Da allora, le cifre stimate pertinenti sono cambiate per via dell'adozione o della prevista adozione di altri atti legislativi.
2. Il 5 marzo 2024 i colegislatori hanno raggiunto un accordo politico preliminare per limitare a 22 milioni di EUR la riassegnazione dall'obiettivo specifico 4 "Competenze digitali avanzate" all'obiettivo specifico 3 "Cibersicurezza e fiducia" del programma Europa digitale prevista nella scheda finanziaria legislativa.
3. Per rispecchiare i termini dell'accordo politico preliminare, la Commissione ha aggiornato la scheda finanziaria legislativa del regolamento sulla cibersolidarietà per quanto riguarda le dotazioni finanziarie per gli obiettivi specifici 2 "Intelligenza artificiale", 3 "Cibersicurezza e fiducia" e "Competenze digitali avanzate", tenendo conto delle riassegnazioni concordate dai colegislatori.
4. Di conseguenza, le dotazioni finanziarie per il periodo 2025-2027 presentate nella scheda finanziaria legislativa aggiornata, fatti salvi i poteri della Commissione nel contesto della procedura di bilancio annuale, sono le seguenti:
   - [544 726 000 EUR] per l'obiettivo specifico 2 "Intelligenza artificiale", tenuto conto della riassegnazione di 65 milioni di EUR all'obiettivo specifico 3 "Cibersicurezza e fiducia";
   - [44 451 000 EUR] per l'obiettivo specifico 3 "Cibersicurezza e fiducia" - parte sotto la gestione diretta della Commissione, compresi i 26 milioni di EUR riassegnati dagli obiettivi specifici 2 e 4;
   - [353 190 613 EUR] per l'obiettivo specifico 3 "Cibersicurezza e fiducia" - parte

---

* L'accordo politico provvisorio ha concluso che la presente dichiarazione della Commissione europea sarà pubblicata nella serie C della Gazzetta ufficiale e che nella serie L figureranno un riferimento e un collegamento alla presente dichiarazione, unitamente all'atto legislativo.

gestita dal Centro europeo di competenza per la cibersicurezza, compresa la riassegnazione di 61 milioni di EUR dagli obiettivi specifici 2 e 4;

- [167 162 423 EUR] per l'obiettivo specifico 4 "Competenze digitali avanzate", tenuto conto della riassegnazione di 22 milioni di EUR all'obiettivo specifico 3 "Cibersicurezza e fiducia".

5. La riserva dell'UE per la cibersicurezza sarà finanziata dalla dotazione finanziaria dell'obiettivo specifico 3 "Cibersicurezza e fiducia" - la parte sotto la gestione diretta della Commissione (che, secondo la scheda finanziaria legislativa aggiornata, è stimata a [44 451 000] EUR)."