

Bruxelles, 22 gennaio 2026
(OR. en)

5611/26

**Fascicolo interistituzionale:
2026/0011 (COD)**

**CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90**

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	21 gennaio 2026
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2026) 11 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")

Si trasmette in allegato, per le delegazioni, il documento COM(2026) 11 final.

All.: COM(2026) 11 final



COMMISSIONE
EUROPEA

Strasburgo, 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• **Motivi e obiettivi della proposta**

Dall'adozione del regolamento sulla cibersicurezza nel 2019, in un contesto geopolitico sempre più complesso, il panorama delle minacce alla cibersicurezza ha registrato una notevole evoluzione¹. Gli attacchi informatici, e in particolare le attività di ransomware, si sono intensificati e sono diventati più sofisticati, prendendo di mira infrastrutture critiche, imprese e il pubblico in generale². Le tecnologie emergenti come l'intelligenza artificiale (IA) e l'informatica quantistica stanno rimodellando gli strumenti di difesa e le tattiche degli avversari. Nella sua relazione del 2024 dal titolo "**The future of European competitiveness**", Mario Draghi ha posto la necessità di aumentare la sicurezza e ridurre le dipendenze tra i principali settori di intervento necessari nell'Unione europea³. Sia la strategia europea per l'Unione della preparazione⁴ che la strategia europea di sicurezza interna (ProtectEU)⁵ hanno posto la cibersicurezza al centro dell'agenda per la resilienza dell'Unione. Tali strategie riconoscono che le minacce persistenti alla cibersicurezza non rappresentano soltanto sfide tecniche, ma anche rischi strategici per la nostra democrazia, la nostra economia e il nostro stile di vita. Analogamente, la comunicazione sul rafforzamento della sicurezza economica dell'UE⁶ individua come obiettivi prioritari impedire l'accesso a informazioni e dati sensibili che potrebbero compromettere la sicurezza economica dell'Unione, nonché prevenire e attenuare le perturbazioni delle infrastrutture critiche dell'Unione che incidono sulla sua economia, ambiti in cui misure di cibersicurezza efficaci svolgono un ruolo cruciale.

In tale contesto, la presente proposta di revisione del regolamento sulla cibersicurezza mira ad affrontare **quattro problemi principali**: i) il disallineamento tra il quadro strategico dell'Unione in materia di cibersicurezza e le esigenze dei portatori di interessi in un panorama delle minacce sempre più ostile; ii) lo stallo nell'attuazione del quadro europeo di certificazione della cibersicurezza; iii) la complessità e la diversità delle politiche in materia di cibersicurezza che incidono sulla postura di cibersicurezza dell'Unione; e iv) l'aumento dei rischi per la sicurezza delle catene di approvvigionamento delle TIC.

Sulla base dei principali problemi individuati, i **due obiettivi generali** dell'intervento sono rafforzare le capacità e la resilienza in termini di cibersicurezza e prevenire la frammentazione nel mercato unico:

- contribuendo a rafforzare la governance della cibersicurezza dell'Unione e a garantire che le istituzioni, le autorità e gli altri portatori di interessi pertinenti siano meglio preparati a prevenire e rilevare le minacce alla cibersicurezza e a reagire in modo coordinato ed efficace; e

¹ ENISA, *ENISA Threat Landscape 2024*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

² ENISA, *ENISA Threat Landscape 2025*.

³ Commissione europea, *The future of European Competitiveness*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20%20A%20competitiveness%20strategy%20for%20Europe.pdf.

⁴ JOIN(2025) 130 final.

⁵ COM(2025) 148 final.

⁶ JOIN(2025) 977 final.

- sostenendo l'elaborazione, l'attuazione e l'adozione di strumenti comuni dell'Unione in materia di cibersicurezza, quali sistemi di certificazione, e fornendo quadri armonizzati che rafforzino la fiducia e l'interoperabilità tra gli Stati membri.

Questi obiettivi generali rispondono alle principali sfide individuate nella definizione del problema. Rispecchiano l'obiettivo strategico generale di rafforzare la governance della cibersicurezza nell'Unione e sostenere lo sviluppo di un mercato unico digitale sicuro, resiliente e competitivo.

Per contribuire al conseguimento degli obiettivi generali sopra elencati, l'intervento persegue gli **obiettivi specifici** seguenti:

- per affrontare il disallineamento tra il quadro strategico dell'Unione in materia di cibersicurezza e le esigenze dei portatori di interessi:
 - OS1: creare la capacità di attuare efficacemente le politiche dell'Unione in materia di cibersicurezza e una costante cooperazione operativa che consenta una cooperazione più strutturata tra gli Stati membri;
 - OS2: sviluppare e attuare mezzi e meccanismi per fornire sostegno e rispondere alle esigenze degli Stati membri, dell'industria e di altri portatori di interessi in modo efficace;
- per far fronte alla scarsa diffusione e alla limitata efficacia del quadro europeo di certificazione della cibersicurezza:
 - OS3: creare i presupposti per una più rapida attuazione di sistemi di certificazione della cibersicurezza sulla base delle esigenze del mercato, ampliando l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza, garantendo un mantenimento efficace e procedure agili, e aumentando la trasparenza;
- per affrontare la frammentazione del panorama della conformità e la complessità dei quadri orizzontali e settoriali:
 - OS4: creare meccanismi e condizioni per facilitare la conformità ai requisiti di cibersicurezza, rendendo in tal modo la loro attuazione più coerente ed efficace.
- per affrontare i rischi di cibersicurezza nella catena di approvvigionamento:
 - OS5: ridurre i rischi per le catene di approvvigionamento critiche delle TIC provenienti da soggetti stabiliti in paesi terzi che destano preoccupazioni per la cibersicurezza o controllati da soggetti di tali paesi terzi (fornitori ad alto rischio) e ridurre le dipendenze critiche sviluppando un quadro coerente ed efficace a livello dell'UE per affrontare i rischi per la sicurezza delle catene di approvvigionamento delle TIC.

La revisione del regolamento sulla cibersicurezza rientra nell'ambito di competenza del **programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione (REFIT)**. Contribuisce in modo significativo a migliorare la chiarezza, a eliminare le inefficienze e ad allineare le procedure tra i quadri giuridici. La revisione del regolamento sulla cibersicurezza contribuisce al corretto funzionamento del mercato interno, garantendo nel contempo la sicurezza e l'autonomia strategica dell'Unione.

Più concretamente, propone una riforma completa del mandato dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornendo un sostegno efficace all'attuazione delle politiche e un valore aggiunto in termini di sostegno alla cooperazione operativa tra gli Stati membri.

Tenuto conto dei rischi e delle sfide crescenti in materia di cibersicurezza che l'Unione si trova ad affrontare, la proposta mira ad aumentare le risorse finanziarie e umane dell'ENISA per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nella difesa dell'ecosistema digitale dell'Unione, affinché l'ENISA possa svolgere in modo efficace i compiti che le sono conferiti dalla presente proposta.

La revisione contribuirà inoltre a eliminare la frammentazione delle pratiche, migliorando il coordinamento e riducendo nel contempo i costi operativi e di conformità a lungo termine. Abrogando l'attuale regolamento sulla cibersicurezza e introducendo un quadro europeo di certificazione della cibersicurezza riformato, la proposta offre uno strumento più efficace ed efficiente che non soltanto promuove la fiducia tra le imprese, il pubblico e le autorità pubbliche ma facilita anche il rispetto della pertinente legislazione dell'Unione. Aumenta l'efficienza rivedendo il modello di governance e sostenendo procedure di certificazione più prevedibili, coerenti e agili per consentire uno sviluppo e un'attuazione più rapidi dei regimi.

Maggiori sinergie con i pertinenti quadri giuridici vigenti dell'Unione promuoveranno la certificazione quale strumento di conformità per le imprese e ridurranno gli oneri amministrativi per gli organismi di valutazione della conformità che operano ai sensi di diversi atti legislativi in materia di cibersicurezza. Inoltre ampliando l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza e consentendo lo sviluppo di un sistema relativo alla postura di cibersicurezza dei soggetti, la proposta riduce i costi di conformità per i soggetti tenuti al rispetto della pertinente normativa dell'Unione in materia di cibersicurezza, a partire dai soggetti che rientrano nell'ambito di applicazione della direttiva NIS 2. Questo approccio semplificherà notevolmente gli obblighi normativi per i soggetti tenuti a soddisfare molteplici requisiti di conformità e garantirà un uso più efficace delle risorse tra le autorità nazionali. Oltre a tale revisione, una proposta di direttiva che introduce modifiche mirate alla direttiva NIS 2 mira a semplificare la conformità e a garantire un'attuazione razionalizzata e coerente di aspetti specifici del quadro in materia di cibersicurezza, anche per quanto riguarda l'ambito di applicazione, le definizioni, la segnalazione di ransomware e la vigilanza dei soggetti che offrono servizi transfrontalieri.

Il nuovo regolamento crea inoltre un quadro armonizzato per affrontare i rischi di natura non tecnica che interessano le catene di approvvigionamento delle TIC, riducendo l'attuale frammentazione degli approcci tra i diversi Stati membri. Nel complesso questi aspetti rappresentano una semplificazione e una modernizzazione sostanziali del quadro giuridico dell'Unione in materia di cibersicurezza, pienamente in linea con i principi di chiarezza, efficienza e preparazione digitale del programma REFIT.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

L'Unione ha ampliato i suoi strumenti giuridici e politici con l'adozione di una serie di strumenti giuridici e misure politiche: i) la direttiva NIS 2 consente di rafforzare la cibersicurezza delle infrastrutture critiche; ii) nella sua "direttiva gemella", la direttiva sulla resilienza dei soggetti critici (CER) sono definite misure di sicurezza fisica; iii) il regolamento sulla ciberresilienza rafforza la cibersicurezza dei prodotti; iv) il regolamento sulla

cibersolidarietà crea capacità di risposta a livello dell'UE; v) il programma dell'UE per la cibersicurezza⁷ sostiene la cooperazione a livello dell'UE in materia di gestione delle crisi, nel cui ambito la Commissione e l'alto rappresentante svolgono un ruolo essenziale nella preparazione e nella risposta agli incidenti di cibersicurezza su vasta scala; vi) il pacchetto di strumenti per la cibersicurezza del 5G (pacchetto di strumenti per il 5G) sostiene la cibersicurezza nelle reti 5G; vii) il piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria⁸ contribuisce a migliorare la loro cibersicurezza; e viii) l'Accademia per le competenze in materia di cibersicurezza⁹ affronta la sfida crescente del divario di talenti nel settore della cibersicurezza.

Il suddetto quadro giuridico in materia di cibersicurezza è stato integrato dalla normativa settoriale, ossia dal regolamento relativo alla resilienza operativa digitale per il settore finanziario, dal codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica per il sottosettore dell'energia elettrica o dalle norme sulla sicurezza delle informazioni (parte IS¹⁰) per il sottosettore del trasporto aereo.

La revisione del regolamento sulla cibersicurezza è allineata alla direttiva NIS 2 e ne rafforza le disposizioni per quanto riguarda il ruolo dell'ENISA nel sostenere l'attuazione della direttiva NIS 2, anche per quanto concerne il sostegno alla cooperazione operativa; è inoltre in linea con il regolamento sulla ciberresilienza, anche per quanto riguarda la panoramica e la gestione delle vulnerabilità in tutto il mercato interno, e aumenta il valore aggiunto della conoscenza situazionale condivisa. Per quanto riguarda il quadro europeo di certificazione della cibersicurezza, la revisione del regolamento sulla cibersicurezza è in linea con il regolamento sulla ciberresilienza per quanto concerne gli obiettivi di sicurezza dei prodotti e la gestione delle vulnerabilità e con il nuovo quadro normativo in materia di accreditamento. Lo sviluppo della certificazione della postura di cibersicurezza per la direttiva NIS 2 crea inoltre una forte sinergia, cui si aggiunge la possibilità di facilitare la conformità con altri atti giuridici pertinenti dell'Unione, come il regolamento generale sulla protezione dei dati (GDPR), senza pregiudicarne le specifiche prescrizioni in materia di certificazione. Inoltre il quadro orizzontale che affronta i rischi di cibersicurezza per le catene di approvvigionamento delle TIC contribuisce all'obiettivo generale della direttiva NIS 2 di creare un livello comune elevato di cibersicurezza nell'Unione e si basa sull'approccio basato sul rischio di tale direttiva.

La revisione del regolamento sulla cibersicurezza, in combinazione con la proposta di direttiva che introduce modifiche mirate alla direttiva NIS 2 a fini di semplificazione, fornisce inoltre gli strumenti necessari per rendere questo quadro complessivo più efficace ed efficiente nel conseguire i risultati attesi, rafforzare la dimensione europea e colmare le restanti lacune normative.

- **Coerenza con le altre normative dell'Unione**

La revisione del regolamento sulla cibersicurezza integrerebbe la direttiva CER, che include considerazioni relative alla catena di approvvigionamento nell'ambito delle misure di resilienza dei soggetti critici. Integrerebbe inoltre prossime iniziative, quali: i) l'atto

⁷ COM(2025) 66 final.

⁸ COM(2025) 10 final.

⁹ COM(2023) 207 final.

¹⁰ Regolamento di esecuzione (UE) 2023/203 della Commissione e regolamento delegato (UE) 2022/1645 della Commissione.

legislativo sullo sviluppo del cloud e dell'IA, che mira, tra l'altro, ad affrontare la mancanza di un'offerta competitiva di servizi di cloud computing a livello dell'Unione su scala sufficiente per servire casi d'uso o settori altamente critici; ii) l'atto legislativo sulle reti digitali; iii) l'imminente revisione del regolamento (UE) 2023/1781¹¹, iv) il quadro in materia di appalti pubblici¹², attualmente in fase di valutazione¹³, e la proposta di regolamento sulla semplificazione della legislazione nel settore del digitale (omnibus digitale)¹⁴ che prevede l'obbligo per l'ENISA di istituire un punto di accesso unico per la segnalazione degli incidenti attraverso il quale i soggetti possano adempiere contemporaneamente agli obblighi di segnalazione degli incidenti previsti da molteplici atti giuridici. La revisione rafforzerebbe inoltre la posizione delle autorità e degli operatori dell'Unione nel dialogo con i partner del Mediterraneo meridionale, in particolare promuovendo l'interconnessione attraverso infrastrutture digitali sicure e affidabili in tutto il Mediterraneo, che è un obiettivo fondamentale del patto per il Mediterraneo.

La revisione del regolamento sulla cibersicurezza è inoltre in linea con i documenti strategici dell'Unione, in particolare per quanto riguarda il quadro in materia di sicurezza delle catene di approvvigionamento delle TIC. Nella strategia ProtectEU la Commissione ha altresì affermato che un approccio armonizzato alla sicurezza della catena di approvvigionamento delle tecnologie dell'informazione e della comunicazione (TIC) può servire per risolvere il problema dell'attuale frammentazione del mercato interno, causata da approcci diversi a livello nazionale, evitare dipendenze critiche e mettere le catene di approvvigionamento TIC al riparo dai fornitori ad altro rischio, garantendo in tal modo la sicurezza delle infrastrutture critiche. La strategia per la sicurezza economica ha inoltre evidenziato la necessità di rendere l'economia e la catena di approvvigionamento dell'UE più resilienti al fine di promuovere la nostra competitività¹⁵. La necessità di affrontare le perturbazioni delle catene di approvvigionamento e gli attacchi informatici è stata sottolineata anche nella strategia per l'Unione della preparazione e nel Libro bianco sulla difesa europea¹⁶. È inoltre in linea con la relazione sul futuro della competitività europea di Mario Draghi, come sottolineato in precedenza. La revisione del regolamento sulla cibersicurezza nel settore della sicurezza delle catene di approvvigionamento delle TIC è altresì coerente con la recente comunicazione congiunta al Parlamento europeo e al Consiglio sul rafforzamento della sicurezza economica dell'UE¹⁷.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La base giuridica della presente proposta è l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). L'articolo 114 TFUE prevede l'adozione di misure volte ad

¹¹ Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio del 13 settembre 2023 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (regolamento sui chip) (GU L 229 del 18.9.2023, pag. 1)

¹² In particolare le direttive 2014/23/UE, 2014/24/UE e 2014/25/UE.

¹³ Commissione europea, "La Commissione pubblica un invito a presentare contributi e una consultazione pubblica sulla valutazione delle direttive sugli appalti pubblici", https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en?prefLang=it&etrans=it.

¹⁴ COM(2025) 837 final.

¹⁵ JOIN(2023) 20 final.

¹⁶ JOIN(2025) 120 final.

¹⁷ COM/2025/977 final.

assicurare l'instaurazione e il funzionamento del mercato interno. Il regolamento (UE) 2019/881 relativo all'ENISA e alla certificazione della cibersecurity per le tecnologie dell'informazione e della comunicazione, comunemente noto come regolamento sulla cibersecurity¹⁸, è stato originariamente adottato a norma di tale disposizione.

Nel settore della cibersecurity in relazione alla sicurezza delle catene di approvvigionamento delle TIC, la frammentazione dei quadri nazionali volti ad affrontare i fattori di rischio di natura non tecnica incide negativamente sul funzionamento del mercato interno, in quanto la divergenza negli approcci nazionali potrebbe, in ultima analisi, far sì che alcuni Stati membri siano maggiormente vulnerabili, con potenziali effetti di ricaduta in tutta l'Unione e ripercussioni sulla resilienza complessiva oltre che sull'affidabilità.

In considerazione della natura dinamica delle minacce alla cibersecurity e della crescente interdipendenza dei sistemi digitali degli Stati membri, l'articolo 114 TFUE rimane la base giuridica giustificata per la revisione del regolamento sulla cibersecurity. La proposta di regolamento tiene conto degli ultimi sviluppi del panorama legislativo in materia di cibersecurity, in particolare in considerazione delle crescenti responsabilità dell'ENISA e dell'ampliamento dell'ambito di applicazione delle certificazioni e della gestione dei rischi.

- **Sussidiarietà (per la competenza non esclusiva)**

Il principio di sussidiarietà impone di valutare la necessità e il valore aggiunto dell'azione dell'Unione. Il rispetto del principio di sussidiarietà in questo settore è già stato riconosciuto all'atto dell'adozione del regolamento sulla cibersecurity attualmente in vigore.

Come già rilevato in relazione al regolamento sulla cibersecurity, l'intervento dell'Unione è fondamentale in quanto le minacce alla cibersecurity e le sfide correlate travalicano i confini dei singoli Stati membri. Soluzioni nazionali frammentate si sono rivelate insufficienti a garantire la fiducia e il coordinamento a livello di mercato. È necessario un quadro giuridico dell'Unione riveduto per eliminare gli ostacoli, garantire un'attuazione uniforme e sostenere gli Stati membri in un contesto sempre più complesso sotto il profilo normativo e in termini di minacce. La cibersecurity è una questione di interesse comune dell'Unione.

Le azioni contemplate dal regolamento proposto offrono un chiaro valore aggiunto favorendo l'armonizzazione, la chiarezza giuridica e contribuendo a dare risposte coordinate alle sfide in materia di cibersecurity.

I compiti attualmente svolti dall'ENISA sono il frutto di un ampliamento avvenuto mediante atti normativi successivi senza una revisione globale delle relative responsabilità principali e risorse. Si sono così create inefficienze e le priorità relative ai compiti fondamentali a sostegno degli Stati membri non sono state definite in modo adeguato. La proposta di intervento mira pertanto a precisare i compiti attuali e a definirne la priorità, al fine di rafforzare il mandato dell'ENISA, consentendole di fungere da punto di competenza unico per la cibersecurity a livello dell'Unione. Su questo punto, non vi è alcuna differenza sostanziale in termini di sussidiarietà rispetto al regolamento sulla cibersecurity. Inoltre la diversità dei sistemi nazionali di certificazione e degli approcci normativi adottati dagli Stati membri crea una frammentazione del mercato e ulteriori oneri di conformità, compromettendo la competitività.

¹⁸ [Regolamento \(UE\) 2019/881 - IT - EUR-Lex.](#)

La nuova proposta prevede inoltre nuovi interventi in relazione alle politiche in materia di catena di approvvigionamento e agli sforzi di semplificazione a livello dell'Unione. Rafforza ulteriormente la sicurezza della catena di approvvigionamento e il settore della cibersecurity all'interno dell'Unione e aumenta la preparazione e la resilienza degli Stati membri e dell'industria.

Se, da un lato, le dipendenze da soggetti stabiliti in un paese terzo che presenta criticità sotto il profilo della cibersecurity o controllati da tale paese terzo, da un soggetto ivi stabilito o da un suo cittadino (fornitori ad alto rischio) interessano soggetti in tutta l'Unione, dall'altro lato, gli incidenti di cibersecurity significativi nella catena di approvvigionamento spesso travalicano i confini nazionali. D'altro canto, data la natura transfrontaliera delle catene di approvvigionamento delle TIC, la frammentazione dei requisiti di conformità nel mercato interno comprometterebbe la certezza del diritto per i soggetti. Peraltro le proposte relative al quadro finanziario pluriennale (QFP) impongono l'esclusione dei fornitori ad alto rischio per tutelare l'integrità del bilancio dell'UE e gli interessi in materia di sicurezza. Il quadro per le catene di approvvigionamento contemplato nel presente regolamento prevede il meccanismo per individuare i paesi che destano preoccupazioni per la cibersecurity, un'attività che può essere svolta efficacemente solo a livello dell'UE. Per quanto riguarda la sicurezza delle catene di approvvigionamento delle TIC, solo un intervento a livello dell'UE garantirà il medesimo livello minimo di sicurezza in tutta l'Unione e la necessaria armonizzazione degli approcci.

La presente revisione mantiene l'obiettivo del regolamento sulla cibersecurity, rafforzandolo ulteriormente. Tale obiettivo non può essere conseguito in misura sufficiente dagli Stati membri, ma può essere conseguito meglio a livello di Unione conformemente all'articolo 5 del trattato sull'Unione europea.

- **Proporzionalità**

Le misure proposte non vanno al di là di quanto necessario per conseguire gli obiettivi strategici della proposta. Inoltre la portata dell'intervento dell'Unione non osta a ulteriori azioni nazionali in materia di questioni di sicurezza nazionale. L'azione dell'Unione è pertanto giustificata in termini di sussidiarietà e proporzionalità.

La proposta intende rispecchiare in modo migliore, sul piano giuridico, il mandato dell'ENISA e il processo per lo sviluppo, l'adozione e il mantenimento dei certificati europei di cibersecurity. La proposta prevede alcuni nuovi compiti per l'ENISA, con l'obiettivo di sostenere gli Stati membri nei settori in cui sono state individuate lacune significative. L'ENISA non sostituirà i CSIRT degli Stati membri. Per quanto riguarda il quadro europeo di certificazione della cibersecurity, la certificazione rimane volontaria e può aiutare i soggetti a dimostrare la conformità ai requisiti di cibersecurity dell'Unione. Questo approccio garantisce il rispetto del principio di proporzionalità.

Per quanto riguarda le soluzioni proposte in relazione alla sicurezza delle catene di approvvigionamento delle TIC, il quadro prevede la raccolta di dati concreti su cosa costituisca una risorsa chiave e su quali misure sarebbero proporzionate e necessarie per garantire la riduzione dei rischi per le catene di approvvigionamento critiche. Prima di definire tali misure, sarà effettuata una valutazione degli impatti economici, che esaminerà, tra l'altro, la fattibilità economica, le alternative disponibili sul mercato e il ciclo di vita dei prodotti specifici. Tale valutazione servirà da base per stabilire quali misure basate sul rischio siano necessarie e più appropriate.

- **Scelta dell'atto giuridico**

La presente proposta riesamina il regolamento (UE) 2019/881, che stabilisce l'attuale mandato e i compiti dell'ENISA e il quadro europeo di certificazione della cibersicurezza. È pertanto opportuno che il mandato riveduto dell'ENISA e le modifiche del quadro europeo di certificazione della cibersicurezza siano stabiliti nell'ambito dello stesso strumento giuridico, segnatamente lo strumento del regolamento. La proposta legislativa prevede inoltre un quadro efficace a livello dell'UE per affrontare i rischi per la sicurezza delle catene di approvvigionamento delle TIC, per il quale un regolamento sarebbe più efficace nell'affrontare i problemi individuati e nel raggiungere gli obiettivi formulati, in quanto solo un intervento a livello dell'UE garantirà lo stesso livello di sicurezza in tutta l'Unione e la necessaria armonizzazione degli approcci. Il processo di recepimento nel caso di una direttiva per questo tipo di intervento potrebbe lasciare un margine di discrezionalità eccessivo a livello nazionale, portando potenzialmente alla mancanza di uniformità di taluni requisiti essenziali di cibersicurezza, all'incertezza giuridica, a un'ulteriore frammentazione o addirittura a situazioni discriminatorie a livello transfrontaliero.

3. **RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO**

- **Valutazioni ex post / Vaglio di adeguatezza della legislazione vigente**

A norma dell'articolo 67 del regolamento (UE) 2019/881, la Commissione europea ha esaminato la pertinenza, l'impatto, l'efficacia, l'efficienza, la coerenza e il valore aggiunto dell'ENISA e del quadro europeo di certificazione della cibersicurezza, tenendo conto dell'evoluzione del panorama tecnologico e normativo. Tale valutazione, completata nel dicembre 2024, ha riguardato il periodo dal 2017 al 2023 e mirava a rivedere il mandato e le attività dell'ENISA e a valutare il ruolo svolto dal quadro europeo di certificazione della cibersicurezza nel promuovere un ambiente informatico sicuro in tutta l'UE. I risultati principali possono essere sintetizzati nel modo seguente.

- **Pertinenza:** la pertinenza dell'ENISA nel settore della cibersicurezza è sottolineata dalla sua capacità di rispondere all'evoluzione delle esigenze dei portatori di interessi e dalla sua adattabilità a un panorama in evoluzione. Sebbene il riscontro dei portatori di interessi sia generalmente positivo, l'impatto dell'ENISA potrebbe essere aumentato. Tale obiettivo può essere conseguito migliorando il sostegno e la visibilità per diversi settori, in particolare le piccole e medie imprese (PMI), che spesso incontrano difficoltà con i requisiti di cibersicurezza. Sono essenziali una migliore organizzazione delle risorse e un coordinamento più chiaro con le autorità nazionali. La ridefinizione delle priorità delle attività e l'ottimizzazione delle risorse renderanno l'ENISA maggiormente allineata alle esigenze dinamiche del panorama europeo della cibersicurezza.

Per quanto riguarda il quadro europeo di certificazione della cibersicurezza, nonostante le promettenti premesse, si ritiene che il suo impatto sia ancora più potenziale che pratico, in quanto è da poco diventato operativo soltanto un sistema di certificazione. Il quadro è concepito per integrarsi senza soluzione di continuità con altri atti giuridici dell'Unione al fine di semplificare le procedure e agevolare gli scambi transfrontalieri. La sua importanza è evidenziata in settori ad alta affidabilità quali i servizi cloud e le infrastrutture 5G.

- **Efficacia:** l'ENISA ha assolto con successo il suo mandato realizzando quasi tutti i risultati previsti e dimostrando flessibilità e resilienza durante crisi quali la pandemia

di COVID-19 e la guerra di aggressione della Russia nei confronti dell'Ucraina. Per aumentare l'efficienza sono necessari una migliore definizione delle priorità, un obiettivo chiaro e un'assegnazione strategica delle risorse. Un approccio più agile alla governance interna è essenziale per adattarsi all'evoluzione delle esigenze della cibersicurezza e ridurre al minimo i ritardi.

Il quadro europeo di certificazione della cibersicurezza è volto ad armonizzare la certificazione della cibersicurezza in tutta l'Unione, ma ha incontrato sfide significative, tra cui limitazioni procedurali e frammentazione, che hanno determinato ritardi e inefficienze, tra cui il ritardo nell'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC). Fattori esterni, come le tensioni geopolitiche e la pandemia di COVID-19, hanno ulteriormente complicato il conseguimento degli obiettivi del quadro europeo di certificazione della cibersicurezza, evidenziando la necessità di misure adattabili e di un'assegnazione coerente delle risorse tra i portatori di interessi per conseguire l'uniformità e l'efficacia nell'ambito della certificazione della cibersicurezza. Nonostante questi ostacoli, si sono registrati risultati positivi, in particolare per quanto riguarda la sensibilizzazione degli Stati membri in merito all'importanza e alle complessità della certificazione della cibersicurezza.

- **Efficienza:** L'ENISA ha operato in modo efficiente nell'ambito della sua struttura organizzativa a matrice, promuovendo la cooperazione e la definizione delle priorità dei compiti. Ha tuttavia incontrato difficoltà nel soddisfare le crescenti richieste e nel coprire posizioni specializzate, rese ancor più gravi da una carenza globale di specialisti informatici, che hanno causato ritardi e un carico di lavoro elevato. Per risolvere tali problemi, l'ENISA potrebbe ottimizzare la propria forza lavoro interna e riassegnare le risorse in modo efficace, come dimostrato da adeguamenti strategici come il trasferimento di risorse verso l'azione di sostegno alla cibersicurezza operato nel 2022. Inoltre il miglioramento della gestione del bilancio e la riduzione delle spese amministrative migliorerebbero ulteriormente l'efficienza operativa dell'Agenzia.

L'efficienza del quadro europeo di certificazione della cibersicurezza è stata oggetto di critiche a causa della proroga dei termini per l'adozione dei sistemi di certificazione della cibersicurezza e delle complessità connesse, che hanno fatto sì che il primo sistema sia stato adottato soltanto all'inizio del 2024, quasi cinque anni dopo l'adozione del regolamento sulla cibersicurezza. Ai ritardi hanno contribuito anche sfide di natura politica e tecnica, come i dibattiti sulla sovranità dei dati e le difficoltà nel tradurre i progetti in atti giuridici. Le sfide politiche e le esigenze tecniche hanno frenato i progressi in tal senso, come si è visto con il sistema europeo di certificazione della cibersicurezza per i servizi cloud (EUCCS) e il sistema per le reti 5G (EU5G). Nonostante queste inefficienze, il quadro ha prodotto diversi risultati positivi. Permane tuttavia la necessità di migliorare il coinvolgimento dei portatori di interessi e la governance interna per garantire un funzionamento ottimale e un contributo strategico.

- **Coerenza:** alla coerenza dell'ENISA contribuiscono un significativo coinvolgimento dei portatori di interessi e l'allineamento ai recenti quadri normativi. Tuttavia, per migliorare la coerenza e l'assegnazione delle risorse, è essenziale migliorare le sinergie con altri organismi dell'Unione, come il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, e con le autorità nazionali. Devono essere inoltre perfezionate la comunicazione interna e la gestione delle risorse all'interno dell'ENISA, così come un'interazione trasparente con i

portatori di interessi privati. Una chiara definizione dei compiti dell'ENISA, coerente con il regolamento sulla ciberresilienza e la direttiva NIS 2, migliorerà sia l'efficienza che la coerenza normativa.

Per quanto riguarda il quadro europeo di certificazione della cibersecurity, la piena coerenza con altri strumenti legislativi dell'Unione, tra cui la direttiva NIS 2 e il regolamento sulla ciberresilienza, è fondamentale per garantire un approccio unificato alla cibersecurity. Sebbene il quadro europeo di certificazione della cibersecurity sia in teoria allineato a tali misure legislative, l'integrazione pratica rimane complessa e richiede un'attenta vigilanza. L'attuazione del sistema EUCC adottato nel quadro del regolamento sulla ciberresilienza sarà un importante test in tal senso.

- **Valore aggiunto dell'UE:** l'ENISA ha contribuito in modo sostanziale all'ecosistema della cibersecurity dell'Unione promuovendo la cooperazione e allineando le pratiche. Il suo ruolo nell'agevolare gli sforzi nazionali e nel fornire informazioni sulle minacce emergenti è stato fondamentale. Tuttavia le critiche dei portatori di interessi del settore privato in merito alla necessità di un sostegno più mirato indicano la necessità di un maggiore coinvolgimento dei portatori di interessi e di una migliore collaborazione dell'industria. Una rivalutazione strategica della gestione delle risorse consentirebbe all'ENISA di adattarsi meglio all'evoluzione delle sfide in materia di cibersecurity e di servire in modo più efficace i diversi portatori di interessi. Il quadro europeo di certificazione della cibersecurity mirava a introdurre processi di certificazione armonizzati, ma ha dovuto affrontare difficoltà di attuazione dovute alla proroga dei termini e alla frammentazione. Il valore aggiunto del quadro europeo di certificazione della cibersecurity è stato limitato a causa delle carenze nel conseguimento dei suoi obiettivi e della mancanza di efficienza. Nonostante tali difficoltà, il quadro europeo di certificazione della cibersecurity ha migliorato l'armonizzazione tra gli Stati membri e creato migliori opportunità di cooperazione, in particolare istituendo forum di cooperazione con i portatori di interessi come il gruppo europeo per la certificazione della cibersecurity (*European Cybersecurity Certification Group – ECCG*).
- **Consultazioni dei portatori di interessi**

Tra il 2023 e il 2025 sono state svolte diverse consultazioni dei portatori di interessi, nel contesto sia della valutazione del regolamento sulla cibersecurity sia della sua revisione, come indicato di seguito.

- **Nel 2023** sono state condotte 65 interviste (di cui 52 più incentrate sull'ENISA e 13 principalmente sul quadro europeo di certificazione della cibersecurity); è stato condotto un programma di indagine, che ha ricevuto 209 risposte (di cui 70 sul quadro europeo di certificazione della cibersecurity); è stata conclusa una consultazione pubblica e sono stati organizzati due seminari sull'analisi SWOT (punti di forza, punti di debolezza, opportunità e rischi) e sulle raccomandazioni, con rispettivamente 26 e 70 partecipanti. Tali attività miravano specificamente a raccogliere i pareri dei portatori di interessi per valutare l'impatto, l'efficacia e l'efficienza dell'ENISA. Nel dicembre 2024 è stata completata la relazione finale dal titolo *Study to Support the Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework carried out for the Commission by PwC, Intellera Consulting and PPMI*, 2024.
- **Nel 2025** la Commissione ha pubblicato un invito a presentare contributi. In particolare, i portatori di interessi sono stati invitati a presentare contributi scritti, tra cui documenti di sintesi, relazioni tecniche o osservazioni su specifiche proposte di riforma. In totale sono

pervenuti 184 contributi individuali da un'ampia gamma di categorie di portatori di interessi, tra cui associazioni di settore, imprese di cibersicurezza, PMI, istituzioni accademiche e organizzazioni di interesse pubblico.

- **Tra aprile e giugno 2025** la Commissione ha organizzato una consultazione pubblica nell'ambito della revisione del regolamento sulla cibersicurezza e ha ricevuto 193 risposte. La consultazione si è articolata in 38 domande, chiuse e aperte, riguardanti il mandato dell'ENISA, il quadro europeo di certificazione della cibersicurezza, la sicurezza delle catene di approvvigionamento delle TIC e la semplificazione.
- **Consultazione mirata (interviste):** È stata condotta una serie di interviste semistruzzate con portatori di interessi selezionati, tra cui rappresentanti dell'ENISA e autorità pubbliche nazionali che hanno sviluppato o che gestiscono piattaforme nazionali di segnalazione. Le interviste si sono concentrate sul ruolo e sulla capacità dell'ENISA, sul funzionamento operativo del quadro europeo di certificazione della cibersicurezza, sulle difficoltà pratiche nell'allineamento dei processi di certificazione a livello nazionale e dell'Unione, sugli oneri di segnalazione e sugli ostacoli all'attuazione. Tali colloqui hanno fornito indicazioni qualitative che hanno arricchito l'interpretazione dei risultati della consultazione pubblica e sono state utili per mettere a punto le opzioni strategiche.
- **Consultazione dei rappresentanti degli Stati membri nel quadro del gruppo di lavoro del Consiglio¹⁹ e nelle discussioni bilaterali,** in cui gli Stati membri hanno potuto esprimere il loro parere sul riesame del regolamento sulla cibersicurezza.
- **Consultazione mirata (gruppi sul quadro europeo di certificazione della cibersicurezza: ECCG, gruppo dei portatori di interessi per la certificazione della cibersicurezza (SCCG)):** La Commissione, in qualità di presidente di entrambi i gruppi, ha presentato lo stato di avanzamento della revisione del regolamento sulla cibersicurezza in occasione delle riunioni dell'ECCG del 12 marzo e del 3 luglio 2025 e della riunione dell'SCCG del 17 marzo 2025. Sono stati inoltre raccolti ulteriori pareri di esperti da parte dei membri dell'ECCG attraverso questionari.

La consultazione si è concentrata su cinque ambiti principali individuati come fondamentali per il futuro funzionamento e la coerenza del quadro dell'Unione in materia di cibersicurezza:

- **mandato e ruolo operativo dell'ENISA**, compreso il sostegno agli Stati membri e le competenze in materia di tecnologie emergenti;
- **efficacia del quadro europeo di certificazione della cibersicurezza**, compresi i processi di governance e di sviluppo;
- **complessità e frammentazione degli obblighi in materia di cibersicurezza**, con particolare attenzione agli oneri di segnalazione e alla potenziale semplificazione;
- **proporzionalità dei requisiti per le PMI** e possibilità di percorsi di conformità differenziati; e
- **impatti sociali ed economici** di norme armonizzate in materia di cibersicurezza, compresi gli effetti sui consumatori, sui diritti, sull'innovazione e sulla competitività.
- **Valutazione d'impatto**

La revisione del regolamento sulla cibersicurezza, unitamente alla proposta di direttiva che introduce modifiche mirate della direttiva NIS 2, è stata sostenuta da una valutazione

¹⁹ Gruppo orizzontale "Questioni riguardanti il ciberspazio".

d'impatto (cfr. la sintesi in appresso). Il comitato per il controllo normativo ha espresso un "parere positivo con riserve" sul progetto di relazione sulla valutazione d'impatto ripresentato relativo alla revisione del regolamento sulla cibersecurity²⁰. La valutazione d'impatto è stata adeguata per tenere conto delle raccomandazioni e delle osservazioni del comitato per il controllo normativo.

La proposta legislativa finale non si discosta dalle conclusioni della valutazione d'impatto.

La Commissione ha esaminato le opzioni in quattro settori di intervento, alla luce degli obiettivi specifici da conseguire: 1) il mandato dell'ENISA (già rientrante nel regolamento sulla cibersecurity vigente); 2) il quadro europeo di certificazione della cibersecurity (già rientrante nel regolamento sulla cibersecurity vigente); 3) modifiche mirate della direttiva NIS 2, il cui obiettivo è la semplificazione, ma che sono anche interconnesse con il mandato dell'ENISA e con il quadro europeo di certificazione della cibersecurity; e 4) la sicurezza della catena di approvvigionamento delle TIC, che è importante anche per l'ecosistema NIS 2 e per il quadro europeo di certificazione della cibersecurity. Ciascuna serie di opzioni rappresenta un settore di intervento a sé stante, pur essendo allo stesso tempo interconnessa e correlata alle altre.

Opzioni per affrontare il disallineamento tra il quadro strategico dell'Unione in materia di cibersecurity e le esigenze dei portatori di interessi in un contesto sempre più ostile

Opzione A.1: *chiarimento del mandato dell'ENISA e definizione delle priorità* – Questa opzione fornirebbe un quadro chiaro e stabile per i compiti dell'ENISA integrando i compiti stabiliti da altri atti legislativi.

Opzione A.2: *riforma del mandato dell'ENISA* – Questa opzione abrogherebbe e sostituirebbe il regolamento sulla cibersecurity, rivedendo il mandato dell'Agenzia.

Opzione A.3: *riforma del mandato dell'ENISA con una forte attenzione al sostegno operativo* – Questa opzione si baserebbe sull'opzione A.2. Inoltre l'ENISA svilupperebbe le capacità per aiutare direttamente, su richiesta di uno Stato membro, i soggetti contemplati dalla direttiva NIS 2 nella risposta e nella ripresa in caso di incidenti di cibersecurity.

Opzioni per il quadro europeo di certificazione della cibersecurity

Opzione B.1: *chiarimento dell'ambito di applicazione, degli elementi e degli obiettivi del quadro europeo di certificazione della cibersecurity e introduzione di un meccanismo di mantenimento* – Questa opzione prevedrebbe un nuovo meccanismo di mantenimento per i sistemi, dopo la loro adozione, che sarà attuato dall'ENISA.

Opzione B.2: *riforma del quadro europeo di certificazione della cibersecurity rivedendone le procedure ed estendendo l'ambito di applicazione per agevolare la semplificazione della conformità normativa* – Questa opzione abrogherebbe il regolamento sulla cibersecurity e lo sostituirebbe con un nuovo regolamento. In aggiunta a quanto previsto dall'opzione B.1, sarebbero riviste anche le procedure relative alla richiesta, allo sviluppo e all'adozione dei sistemi per migliorare la rendicontabilità e l'efficienza.

Opzione B.3: *riforma del quadro europeo di certificazione della cibersecurity come previsto dall'opzione B.2 e introduzione di una certificazione obbligatoria per la postura di cibersecurity* – Questa opzione si baserebbe sull'opzione B.2, ma mira a potenziare

²⁰ Regolamento (UE) 2019/881 (<http://data.europa.eu/eli/reg/2019/881/oj>).

ulteriormente l'impatto del quadro introducendo la certificazione obbligatoria dei soggetti essenziali tenendo conto di scenari di rischio specifici, invece di fare esclusivamente affidamento sulla certificazione volontaria dei soggetti.

Opzioni di semplificazione

Opzione C.1: *adozione di un approccio basato su strumenti non legislativi e non vincolanti, compreso il ricorso ai poteri esistenti (adozione di atti di esecuzione a norma dell'articolo 21, paragrafo 5, e dell'articolo 23, paragrafo 11, della direttiva NIS 2)* – Questa opzione prevede l'adozione di atti di esecuzione utilizzando i poteri esistenti a norma della direttiva NIS 2 per garantire un livello più elevato di armonizzazione delle misure di gestione dei rischi di cibersicurezza, delle soglie per la segnalazione degli incidenti, nonché del tipo di informazioni, dei formati e della procedura di notifica. Prevede inoltre l'adozione di una serie di orientamenti per rafforzare la certezza del diritto e un'attuazione armonizzata.

Opzione C.2: *intervento mirato: ulteriore semplificazione della conformità al pertinente quadro normativo dell'Unione in materia di cibersicurezza* – Questa opzione comporta un intervento limitato attraverso modifiche del regolamento sulla cibersicurezza e della direttiva NIS 2 con l'obiettivo di semplificare aspetti specifici del quadro in materia di cibersicurezza, tra cui adeguamenti dell'ambito di applicazione, massima armonizzazione per gli atti di esecuzione, prova della conformità attraverso la certificazione, e adozione della serie di orientamenti di cui all'opzione C.1.

Opzione C.3: *armonizzazione delle misure relative alla cibersicurezza stabilite nella normativa dell'Unione* – Questa opzione si baserebbe sull'opzione C.2 e eliminerebbe tutte le misure di gestione dei rischi di cibersicurezza incluse nella normativa settoriale e i poteri conferiti in relazione a tali misure. L'ecosistema della direttiva NIS 2 sarebbe invece modificato per prevedere obblighi semplificati per tutti i tipi di soggetti, con l'obiettivo di promuovere l'armonizzazione.

Opzioni per la sicurezza delle catene di approvvigionamento delle TIC

Opzione D.1: *adozione di un approccio non vincolante per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC* – Questa opzione non prevedrebbe un intervento normativo a livello dell'UE. La Commissione aumenterebbe invece il numero di valutazioni coordinate del rischio e di pacchetti di strumenti volontari.

Opzione D.2: *intervento normativo ad hoc che codifica il pacchetto di strumenti per il 5G* – Questa opzione codificherebbe le misure del pacchetto di strumenti per il 5G. Introdurrebbe l'obbligo per gli Stati membri di provvedere affinché nelle risorse chiave della rete non siano utilizzati componenti di fornitori ad alto rischio.

Opzione D.3: *quadro globale e orizzontale per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC* – Questa opzione istituirebbe un quadro normativo orizzontale, neutro dal punto di vista tecnologico e settoriale, per affrontare i rischi di cibersicurezza di natura non tecnica nelle catene di approvvigionamento delle TIC.

Dopo un'analisi approfondita, il pacchetto strategico prescelto è risultato la seguente combinazione di opzioni: opzione A.2 (riforma del mandato dell'ENISA); opzione B.2 (riforma del quadro europeo di certificazione della cibersicurezza rivedendone le procedure ed estendendo l'ambito di applicazione per agevolare la semplificazione della conformità normativa); e l'opzione C.2 (intervento mirato: ulteriore semplificazione della conformità al pertinente quadro normativo dell'Unione in materia di cibersicurezza) e l'opzione D.3 (quadro

globale e orizzontale per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC).

Questa combinazione offre una risposta ben equilibrata alle sfide politiche individuate, migliorando in modo significativo l'efficacia, l'efficienza e la coerenza in tutta l'Unione.

La transizione verso l'opzione prescelta proposta per il quadro normativo comporterà costi, sia per l'ENISA, per lo svolgimento dei suoi nuovi compiti (stimati in 161,3 milioni di EUR nell'arco di cinque anni), sia per le autorità pubbliche in tutta l'Unione, per la vigilanza (stimati in 80 milioni di EUR nell'arco di cinque anni, tenendo conto dei pertinenti risparmi sui costi). Per quanto riguarda le imprese, nell'arco di cinque anni l'eliminazione graduale di specifiche apparecchiature ad alto rischio potrebbe comportare costi annui compresi tra 3,4 e 4,3 miliardi di EUR per gli operatori di reti mobili, mentre gli investimenti in fornitori affidabili potrebbero aumentare fino a 2 miliardi di EUR all'anno.

Allo stesso tempo, grazie alla semplificazione e alla riduzione degli obblighi di conformità sono attesi risparmi sui costi fino a 15,3 miliardi di EUR per le imprese nell'arco di cinque anni. Inoltre il miglioramento della postura di cibersicurezza complessiva dell'Unione e della sua sovranità tecnologica e l'incentivazione dell'innovazione e della competitività produrrebbero notevoli vantaggi per i cittadini, le autorità pubbliche e le imprese. Si prevede che nel lungo periodo ciò compenserà in larga misura le spese iniziali.

Riducendo la frammentazione del mercato e armonizzando i requisiti normativi, le opzioni prescelte rafforzano la parità di concorrenza in tutta l'Unione, offrendo alle imprese percorsi più chiari verso la conformità e l'innovazione.

Le opzioni prescelte contribuirebbero inoltre alla semplificazione attraverso orientamenti chiari e sistemi integrati, riducendo gli oneri amministrativi. Le opzioni rispettano il principio "one in, one out" garantendo che i nuovi obblighi siano controbilanciati da riduzioni introdotte altrove.

- **Efficienza normativa e semplificazione**

La revisione del regolamento sulla cibersicurezza, attraverso le opzioni strategiche selezionate A.2, B.2, C.2 e D.3, contribuisce in misura sostanziale a migliorare la chiarezza, a eliminare le inefficienze e ad allineare le procedure tra i quadri giuridici. Più concretamente, l'opzione A.2 propone una riforma completa del mandato dell'ENISA, sostenendo efficacemente l'attuazione delle politiche e la cooperazione operativa tra gli Stati membri. Tale consolidamento contribuirà inoltre a eliminare la frammentazione delle pratiche, migliorando il coordinamento e riducendo nel contempo i costi di conformità e operativi a lungo termine. L'opzione B.2, che prevede l'abrogazione dell'attuale regolamento sulla cibersicurezza e l'introduzione di un quadro europeo di certificazione della cibersicurezza riformato, aumenta l'efficienza rivedendo il modello di governance e sostenendo procedure di certificazione più prevedibili, coerenti e agili. Ciò consentirà un'adozione più rapida dei sistemi e un migliore allineamento alla legislazione trasversale, riducendo la frammentazione normativa e alleggerendo l'onere per i portatori di interessi sia del settore pubblico che di quello privato. L'opzione C.2 riduce i costi di conformità per i soggetti tenuti al rispetto della pertinente normativa dell'Unione in materia di cibersicurezza attraverso modifiche dell'ambito di applicazione e consentendo sistemi organizzativi di certificazione della cibersicurezza per i soggetti che rientrano nell'ambito di applicazione della direttiva NIS 2 e di altri atti giuridici. Questo approccio semplificherà notevolmente gli obblighi normativi per i soggetti tenuti ad adempiere a una molteplicità di prescrizioni e garantirà un uso più efficace delle risorse tra le autorità nazionali. L'opzione D.3 crea un quadro armonizzato per affrontare i rischi di natura non

tecnica che interessano le catene di approvvigionamento delle TIC, riducendo l'attuale frammentazione degli approcci tra gli Stati membri. Insieme, queste opzioni rappresentano una semplificazione e una modernizzazione sostanziali del quadro giuridico dell'Unione in materia di cibersicurezza, pienamente in linea con i principi REFIT di chiarezza, efficienza e preparazione digitale.

La proposta è coerente con la "verifica digitale", in quanto la particolare attenzione riservata alla razionalizzazione dei processi digitali dimostra l'impegno dell'Unione a favore di un approccio che privilegi la digitalizzazione e garantisca uno scambio di dati e un processo decisionale più rapidi e affidabili. Anche l'opzione D.3 potrebbe avere un forte impatto sulla digitalizzazione, in quanto comporterebbe la sostituzione di componenti provenienti da soggetti stabiliti in paesi terzi che destano preoccupazioni per la cibersicurezza o controllati da soggetti di tali paesi terzi (fornitori ad alto rischio).

- **Diritti fondamentali**

La proposta legislativa è stata valutata sulla base del suo potenziale di rafforzare o mettere a rischio i diritti fondamentali e di promuovere l'uguaglianza e la fiducia, con particolare attenzione agli impatti e ai diritti sociali, tra cui la vita privata, la protezione dei dati e alla capacità dei singoli di comprendere, esercitare e far valere i propri diritti.

L'estensione del mandato dell'ENISA contribuirà a rafforzare la ciberresilienza di tutta l'economia e della società in generale, determinando una migliore protezione della vita privata e dei dati personali delle persone. La proposta sosterrà inoltre l'istruzione e la formazione in materia di cibersicurezza, in quanto chiarisce il ruolo dell'ENISA nello sviluppo di competenze per la forza lavoro nel settore della cibersicurezza.

Il quadro europeo di certificazione della cibersicurezza rafforzerà inoltre la fiducia dei cittadini e delle imprese dell'Unione in soluzioni TIC certificate che facilitano la vita quotidiana. L'introduzione di ulteriori sistemi aumenterebbe tale impatto.

La proposta contribuisce alla fiducia delle persone incentivando i soggetti di settori critici a ottenere la certificazione della cibersicurezza, dimostrando così pubblicamente il loro livello elevato di cibersicurezza. Inoltre, garantendo la segnalazione armonizzata degli incidenti di ransomware e adottando misure per la transizione verso la crittografia post-quantistica, essa aumenterebbe la fiducia del pubblico nella protezione dei dati sensibili in settori critici.

Le disposizioni relative alla sicurezza della catena di approvvigionamento avranno un certo impatto sulla protezione dei diritti fondamentali limitando le ingerenze straniere. Attività quali lo spionaggio e la sorveglianza ledono gravemente i diritti fondamentali dei cittadini. Tale quadro orizzontale avrebbe il potenziale per migliorare la fiducia, la sicurezza e la tutela della vita privata in varie tecnologie e soluzioni digitali.

4. INCIDENZA SUL BILANCIO

Il bilancio stimato dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), che contribuirà a un aumento significativo della sicurezza dell'UE, è stato stimato pari a 341 milioni di EUR per 7 anni, corrispondente a un bilancio medio annuo di 49 milioni di EUR (proiezioni per il periodo 2028-2034). Si tratta di un aumento dell'81,5 % del bilancio dell'Agenzia nel 2025. I benefici generati dall'iniziativa proposta, analizzati nella valutazione d'impatto, saranno significativi, con un risparmio sui costi a carico delle imprese fino a 14,6 miliardi di EUR. Inoltre, sebbene l'entità dei potenziali risparmi sui costi connessi al miglioramento generale della preparazione dell'Unione agli incidenti di cibersicurezza sia per

sua natura difficile da quantificare, si stima che i risparmi sui costi legati a una maggiore rapidità della risposta e al rallentamento della proliferazione degli incidenti di cibersicurezza potrebbero variare da 3,7 a 4,4 miliardi di EUR nell'arco di cinque anni. Nel contesto delle prossime iniziative politiche, la Commissione esaminerà la distribuzione complessiva delle risorse tra le istituzioni, gli organi, le agenzie e gli uffici europei nel settore della cibersicurezza e al loro interno, al fine di sfruttare le conoscenze e le competenze e individuare e sviluppare sinergie.

Le risorse aggiuntive proposte per rafforzare l'Agenzia si traducono in 118 equivalenti a tempo pieno (ETP) e costi operativi aggiuntivi che copriranno gli attuali accordi di contributo tra l'ENISA e la Commissione, come la manutenzione della piattaforma unica di segnalazione; gli ETP che lavorano al funzionamento e all'amministrazione della riserva dell'UE per la cibersicurezza, nonché importanti iniziative della Commissione come l'istituzione del punto di accesso unico nell'ambito della proposta "omnibus digitale". Altri costi operativi riguardano il programma di divulgazione coordinata delle vulnerabilità, la raccolta e l'intelligence sulle minacce alla cibersicurezza, la sicurezza delle comunicazioni e lo sviluppo della maturità in materia di cibersicurezza per l'ENISA. A questa stima si aggiungono anche i costi operativi per il mantenimento dei sistemi europei di certificazione della cibersicurezza, le autorizzazioni relative alle competenze in materia di cibersicurezza e il servizio relativo agli strumenti di prova, costi che però prevedono anche meccanismi di autofinanziamento tramite la riscossione di diritti.

Un aspetto importante della proposta è l'introduzione di meccanismi di riscossione di diritti che, tra gli altri obiettivi strategici, contribuiranno anche a un circuito finanziario sostenibile all'interno dell'Agenzia. Il regolamento sulla cibersicurezza riveduto presenta tre tipi di diritti che contribuiranno al bilancio dell'ENISA, vale a dire i diritti per il rilascio di autorizzazioni per le attestazioni delle competenze, i diritti per il servizio relativo agli strumenti di prova e i diritti per il sostegno al mantenimento dei sistemi europei di certificazione della cibersicurezza. I benefici previsti per il bilancio dell'UE sono stimati a circa 18,5 milioni di EUR nell'arco di un periodo di 7 anni, dal 2028 al 2034.

La richiesta di bilancio della Commissione si traduce in 50 posti ETP supplementari, per l'attuazione del quadro per le catene di approvvigionamento e l'esecuzione dei compiti relativi, tra l'altro, all'elaborazione di atti di esecuzione per i meccanismi di riscossione di diritti, al mantenimento dei sistemi di certificazione, alla normazione e al sostegno alla cooperazione operativa. Si stima che il costo a carico della Commissione per l'attuazione del quadro per le catene di approvvigionamento risentirà in modo specifico del numero di valutazioni dell'assetto proprietario e di controllo che saranno effettuate dalla Commissione. I risultati di questo compito contribuiranno tuttavia notevolmente ai risparmi per gli Stati membri in sede di supervisione dell'attuazione delle misure di attenuazione e degli obblighi imposti dal quadro ai soggetti rientranti nell'ambito di applicazione della direttiva NIS 2. Gli Stati membri saranno in grado di sfruttare direttamente i risultati delle valutazioni del controllo della proprietà, anziché spendere individualmente risorse per le stesse esigenze di valutazione.

Per informazioni più dettagliate si veda la scheda finanziaria che accompagna il pacchetto sulla cibersicurezza.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La Commissione monitorerà l'applicazione del regolamento proposto e ogni cinque anni presenterà al Parlamento europeo e al Consiglio una relazione sulla sua valutazione. Queste relazioni saranno rese pubbliche e illustreranno in dettaglio l'effettiva applicazione del regolamento proposto.

- **Documenti esplicativi (per le direttive)**

Non applicabile in quanto la proposta è un regolamento.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

La proposta chiarisce il ruolo dell'ENISA e le affida compiti concreti per fornire sostegno ai relativi portatori di interessi, tra cui al primo posto vi sono gli Stati membri, in particolare per quanto riguarda il sostegno all'attuazione delle politiche e della normativa dell'Unione, la cooperazione operativa, lo sviluppo di capacità, la certificazione della cibersecurity e la normazione nonché il miglioramento della forza lavoro nel settore della cibersecurity e della sua mobilità in tutta l'Unione. La proposta mira inoltre a rendere il quadro europeo di certificazione della cibersecurity più efficace ed efficiente per migliorare il livello di cibersecurity all'interno dell'Unione e a fornire ai consumatori gli strumenti per operare scelte informate quando acquistano prodotti, servizi, processi TIC e servizi di sicurezza gestiti nel mercato interno. Inoltre, in combinazione con la proposta di direttiva che introduce modifiche mirate alla direttiva NIS 2, la presente proposta mira ad agevolare il rispetto degli obblighi in materia di cibersecurity e a sbloccare risorse per rafforzare la preparazione operativa in materia di cibersecurity dei soggetti nei settori critici dell'Unione. Infine, la proposta risponde alla necessità di rendere l'economia e la catena di approvvigionamento delle TIC dell'Unione più resilienti al fine di promuovere la propria sicurezza e competitività. I dettagli sono forniti di seguito.

TITOLO I: DISPOSIZIONI GENERALI

Il titolo I del regolamento proposto contiene le disposizioni generali: l'oggetto (articolo 1) e le definizioni (articolo 2), compresi i riferimenti alle pertinenti definizioni di altri strumenti dell'Unione, quali la direttiva (UE) 2022/2555²¹ (direttiva NIS 2), il regolamento (CE) n. 765/2008²² e il regolamento (UE) n. 1025/2012²³.

TITOLO II: ENISA (AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA)

Il titolo II del regolamento proposto contiene le disposizioni fondamentali relative all'ENISA.

Il capo I definisce la missione (articolo 3) e gli obiettivi dell'ENISA (articolo 4).

Al capo II sono illustrati i compiti dell'Agenzia, che si articolano in tre sezioni.

La sezione 1 contiene disposizioni relative ai compiti connessi al sostegno dell'attuazione delle politiche e del diritto dell'Unione. Specifica quali soggetti e organizzazioni devono

²¹ <http://data.europa.eu/eli/dir/2022/2555/oj>.

²² <http://data.europa.eu/eli/reg/2008/765/oj>.

²³ <http://data.europa.eu/eli/reg/2012/1025/oj>.

ricevere sostegno e il modo in cui ciò dovrebbe avvenire (articolo 5). L'articolo 6 definisce le responsabilità dell'Agenzia in materia di sviluppo delle capacità, tra cui l'offerta di conoscenze e competenze agli Stati membri in materia di prevenzione e contrasto delle minacce informatiche, l'aggiornamento delle strategie di cibersicurezza e l'espansione della forza lavoro nel settore della cibersicurezza. L'ENISA assisterà inoltre gli Stati membri nelle loro attività di sensibilizzazione (articolo 7), effettuerà analisi delle principali tendenze del mercato in materia di cibersicurezza e diffonderà consulenze e analisi tecniche (articolo 8). L'ENISA contribuirà inoltre alla cooperazione internazionale in materia di cibersicurezza e la promuoverà, come descritto all'articolo 9.

La sezione 2 definisce i compiti dell'ENISA per quanto riguarda la cooperazione operativa in relazione agli Stati membri, ai soggetti dell'Unione e al servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione (CERT-UE), alla rete di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) e ad altri portatori di interessi, compresa la pubblicazione di orientamenti e l'attuazione di strumenti di comunicazione sicura (articolo 10). L'ENISA contribuirà inoltre a migliorare la conoscenza situazionale in materia di minacce e incidenti informatici, (tra l'altro) sviluppando uno o più archivi di intelligence sulle minacce informatiche, effettuando analisi ed emettendo allerte precoci (articolo 11). Le norme relative a tali allerte precoci (contenuto, tempistica, servizio) sono stabilite all'articolo 12. Per assistere i soggetti essenziali e importanti nella preparazione e nella risposta agli incidenti di ransomware, nonché nella ripresa dagli stessi, l'ENISA gestisce la riserva dell'UE per la cibersicurezza secondo le modalità esposte all'articolo 13 e in cooperazione con Europol e i CSIRT o altre autorità competenti, a seconda dei casi. L'articolo 14 contiene disposizioni sul ruolo dell'ENISA nelle esercitazioni di cibersicurezza a livello dell'Unione, compresa l'elaborazione di un programma continuo annuale di esercitazioni di cibersicurezza a livello dell'Unione. Oltre a tali compiti, l'ENISA dovrebbe fornire strumenti e piattaforme, in particolare la piattaforma unica di segnalazione istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 (articolo 15). Infine l'Agenzia deve sviluppare una capacità comune di servizi per la gestione delle vulnerabilità dell'Unione e fornire servizi di gestione delle vulnerabilità (articolo 16).

La sezione 3 sulla certificazione della cibersicurezza e la normazione definisce i compiti dell'Agenzia a tale riguardo. L'articolo 17 descrive il ruolo dell'ENISA nello sviluppo e nell'attuazione del quadro europeo di certificazione della cibersicurezza, compreso il suo ruolo guida nella preparazione dei sistemi e nel garantirne il mantenimento nonché nello sviluppo delle capacità, mentre l'articolo 18 stabilisce in che modo l'ENISA dovrebbe impegnarsi nell'elaborazione di specifiche tecniche e contribuire alle attività di normazione a livello europeo e internazionale, anche nel settore degli algoritmi crittografici.

La sezione 4 illustra in dettaglio i compiti dell'Agenzia per quanto riguarda l'attuazione dell'Accademia per le competenze in materia di cibersicurezza. L'articolo 19 contiene disposizioni relative al ruolo dell'ENISA per quanto riguarda il quadro europeo delle competenze in materia di cibersicurezza (European cybersecurity skills framework – ECSF), mentre i suoi compiti relativi allo sviluppo e al mantenimento di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza sono stabiliti all'articolo 20. I requisiti per diventare un fornitore autorizzato di attestati sono stabiliti all'articolo 21 mentre le prescrizioni relative al trattamento delle domande sono definite all'articolo 22. L'ENISA deve mettere a disposizione del pubblico informazioni relative all'ECSF e agli attestati delle competenze individuali in materia di cibersicurezza (articolo 23).

Il capo III riguarda l'organizzazione dell'ENISA. La struttura amministrativa e di gestione dell'Agenzia comprende anche un vicedirettore esecutivo (articolo 24). Le disposizioni relative al consiglio di amministrazione, alla sua composizione, al suo presidente, alle riunioni, alle funzioni e alle modalità di voto sono contenute nella sezione 1 (articoli a 25 a 29). Il comitato esecutivo assiste il consiglio di amministrazione come stabilito all'articolo 30 nella sezione 2. La sezione 3 comprende le norme relative alla nomina, alla rimozione dall'incarico e alla proroga del mandato del direttore esecutivo (articolo 31) e le norme relative ai suoi compiti e responsabilità (articolo 32). Il consiglio di amministrazione può decidere di istituire un ruolo di vicedirettore esecutivo per assistere il direttore esecutivo (sezione 4, articoli 33 e 34). Il consiglio di amministrazione deve istituire il gruppo consultivo ENISA, che deve fornire consulenza all'ENISA conformemente alle disposizioni di cui all'articolo 35. La sezione 6 stabilisce le norme relative alla creazione e alla composizione della commissione di ricorso (articolo 36) e ai suoi membri (articolo 37). L'articolo 38 specifica le circostanze in cui i membri della commissione di ricorso devono astenersi dal prendere parte a un procedimento di ricorso e illustra i motivi per cui un membro della commissione può essere ricusato. Si può presentare ricorso presso la commissione di ricorso avverso le decisioni prese dall'ENISA o in caso di suo mancato intervento (articolo 39). L'articolo 40 contiene disposizioni sulle persone legittimate a presentare ricorso, sui termini e sulla forma del ricorso. Gli articoli da 41 a 43 disciplinano la revisione precontenziosa, l'esame delle decisioni sui ricorsi e i ricorsi dinanzi alla Corte di giustizia. Infine l'articolo 44 regola il processo relativo al documento unico di programmazione.

Il capo IV riguarda la formazione e la struttura del bilancio dell'Agenzia, nonché le regole che ne disciplinano l'esecuzione (articoli da 45 a 55). Esso contiene anche le disposizioni per facilitare la lotta contro la frode, la corruzione e altre attività illecite (articolo 51).

Il capo V riguarda il personale dell'Agenzia e comprende disposizioni generali relative allo statuto dei funzionari e al regime applicabile agli altri agenti, nonché le regole che disciplinano i privilegi e le immunità (articoli 56 e 57). Esso introduce disposizioni che impongono agli Stati membri di designare funzionari di collegamento quali esperti nazionali distaccati presso l'ENISA definendone il ruolo in seno all'Agenzia (articolo 58). Comprende inoltre disposizioni che disciplinano il ricorso a esperti nazionali distaccati e ad altro personale non alle dipendenze dell'Agenzia (articolo 59).

Infine, il capo VI contiene le disposizioni generali relative all'Agenzia. Ne definisce lo status giuridico (articolo 60), ne stabilisce la sede (articolo 61) e contiene disposizioni concernenti all'accordo sulla sede e le condizioni operative dell'Agenzia, nonché il controllo amministrativo da parte del Mediatore (articoli 62 e 63). Esso include disposizioni che disciplinano le questioni di responsabilità, il regime linguistico e la protezione dei dati personali (articoli da 64 a 66), nonché le norme di sicurezza in materia di protezione delle informazioni sensibili non classificate e di quelle classificate (articolo 67). Stabilisce norme per la cooperazione con i soggetti dell'Unione e le autorità nazionali (articolo 68) e con altri portatori di interessi (articolo 69). Esso descrive le regole che disciplinano la cooperazione dell'Agenzia con i paesi terzi e le organizzazioni internazionali (articolo 70).

TITOLO III: QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Il titolo III del regolamento proposto istituisce il quadro europeo di certificazione della cibersecurity.

Il capo I introduce gli obiettivi, l'ambito di applicazione e le procedure del quadro. Gli obiettivi (articolo 71) comprendono il rafforzamento della cibersicurezza in tutta l'Unione e l'agevolazione di un approccio armonizzato alla certificazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersicurezza dei soggetti. Il quadro dovrebbe inoltre sfruttare la certificazione per semplificare la conformità alla normativa applicabile dell'Unione attraverso la presunzione di conformità, riducendo in tal modo gli oneri per le imprese (articolo 78). Il capo I illustra poi gli aspetti procedurali, a cominciare dalle consultazioni sulle priorità strategiche in materia di certificazione europea della cibersicurezza e dalla pubblicazione delle informazioni relative all'elaborazione del sistema da parte della Commissione, nonché dalla creazione di una nuova assemblea europea sulla certificazione della cibersicurezza (articolo 72). A seguito di una richiesta dettagliata della Commissione (articolo 73), l'ENISA dovrebbe presentare una proposta di sistema entro 12 mesi. L'articolo 74 prevede termini aggiuntivi relativi alla trasmissione del parere dell'ECCG e alla presentazione del sistema in vista della sua adozione da parte della Commissione. L'articolo 75 introduce un chiaro meccanismo di mantenimento per i sistemi esistenti, che potrebbe portare al loro riesame (articolo 76). Il riesame di un sistema potrebbe basarsi inoltre su una valutazione periodica della sua efficacia e del suo impatto sul mercato unico. L'articolo 77 fornisce all'ENISA una base per elaborare specifiche tecniche a sostegno dello sviluppo e del mantenimento dei sistemi europei di certificazione della cibersicurezza. In sede di adozione o riesame di un regime, la Commissione può includere riferimenti a tali specifiche tecniche (articolo 74). Le varie procedure garantiscono la trasparenza e la qualità dei risultati coinvolgendo esperti e comuni portatori di interessi nelle varie fasi della pianificazione, dello sviluppo, dell'adozione e del mantenimento dei sistemi di certificazione. L'articolo 79 prevede un apposito sito web dell'ENISA sui sistemi europei di certificazione della cibersicurezza, che dovrebbe fornire informazioni sui sistemi adottati, nonché sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità rilasciati nell'ambito di tali sistemi.

Il capo II stabilisce le norme generali per il contenuto dei sistemi europei di certificazione della cibersicurezza.

L'articolo 80 stabilisce un elenco di obiettivi di sicurezza che devono essere rispettati dal sistema progettato dall'ENISA e garantisce l'allineamento alla normativa pertinente in materia di cibersicurezza. Ciascun sistema europeo di certificazione della cibersicurezza può prevedere gli elementi specificati all'articolo 81. Tali elementi devono essere compatibili con la normativa dell'Unione e possono essere armonizzati tra i vari sistemi ricorrendo a disposizioni tipo. Entrambe le disposizioni prevedono la flessibilità necessaria per adattarsi ai diversi tipi di sistemi. Ulteriori disposizioni specificano le norme relative ai livelli di affidabilità (articolo 82) e all'autovalutazione della conformità (articolo 83). Il capo stabilisce inoltre un elenco di informazioni supplementari (articolo 84) che il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC deve mettere a disposizione.

Infine, il capo III stabilisce le norme di governance per il quadro europeo di certificazione della cibersicurezza, suddivise in tre sezioni.

La sezione 1 riguarda le norme relative al rilascio di certificati europei di cibersicurezza, compresi quelli con un livello di affidabilità "elevato" (articolo 85). Stabilisce inoltre le norme per l'armonizzazione dei sistemi europei di certificazione della cibersicurezza con i sistemi nazionali di certificazione della cibersicurezza e i certificati di cibersicurezza nazionali (articolo 86) e prevede la possibilità di riconoscimento internazionale dei certificati europei di cibersicurezza, sulla base del principio di equivalenza (articolo 87). La sezione

definisce inoltre il ruolo delle autorità nazionali di certificazione della cibersecurity e le relative norme applicabili (articolo 88) e stabilisce le norme per un meccanismo di revisione tra pari tra tali autorità, garantendo norme equivalenti in tutta l'Unione (articolo 89), nonché per la cooperazione tra tali autorità in seno all'ECCG (articolo 90).

La sezione 2 prevede quanto segue: i) norme armonizzate in materia di accreditamento e autorizzazione degli organismi di valutazione della conformità (articoli da 91 a 92); ii) norme in materia di notifica, compreso il conferimento di poteri al fine di garantire un ulteriore allineamento al pertinente diritto dell'Unione e al nuovo quadro legislativo (articolo 93); e iii) una procedura di contestazione (articolo 94) che garantisca il rispetto dei requisiti per gli organismi di valutazione della conformità.

Infine, la sezione 3 prevede diritti e ricorsi giurisdizionali contro le decisioni relative alla certificazione (articolo 96) e impone agli Stati membri di stabilire e applicare sanzioni proporzionate in caso di violazioni della regolamentazione.

TITOLO IV

Il capo I, articolo 98, definisce l'ambito di applicazione del quadro per catene di approvvigionamento delle TIC affidabili. Il quadro affronterà i rischi di natura non tecnica nei settori ad alta criticità e in altri settori critici di cui alla direttiva (UE) 2022/2555. Il meccanismo individua le risorse TIC chiave nelle catene di approvvigionamento critiche delle TIC e stabilisce misure di attenuazione adeguate e proporzionate al tipo di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555. Il quadro si baserà su valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza, richieste dalla Commissione o da almeno tre Stati membri. L'articolo 99 specifica in che modo tali valutazioni dei rischi saranno effettuate, precisando che dovrebbero anche stabilire misure di attenuazione. Tali valutazioni dei rischi dovrebbero essere completate entro sei mesi dalla richiesta. Su richiesta della Commissione, il gruppo di cooperazione NIS può concordare un periodo più breve. Il quadro prevede la possibilità di una procedura di emergenza se un intervento immediato è giustificato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che sussista una minaccia informatica significativa per la sicurezza dell'Unione in relazione alle catene di approvvigionamento critiche delle TIC. In tal caso, la Commissione consulta gli Stati membri sulla necessità di adottare una o più misure di attenuazione ed effettua una valutazione dei rischi. L'articolo 100 stabilisce che se, a seguito della valutazione dei rischi di cui all'articolo 99 o sulla base di altre fonti, come una dichiarazione pubblica a nome dell'Unione o di uno Stato membro, risulta che un paese terzo presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione verifica la minaccia rappresentata da tale paese, tenendo conto degli elementi elencati all'articolo 100. Qualora la Commissione concluda che un paese terzo presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, l'articolo 100 prevede una procedura che consente alla Commissione di designare tale paese terzo come paese che desta preoccupazioni per la cibersecurity delle catene di approvvigionamento delle TIC. I soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersecurity designato a norma di questo articolo, o controllati da tale paese terzo, da un soggetto ivi stabilito o da un suo cittadino, non saranno autorizzati a svolgere una serie di attività specificate in tale articolo. L'articolo 101 prevede un meccanismo generale per la catena di approvvigionamento delle TIC in base al quale, una volta completata la valutazione dei rischi per la sicurezza da parte del gruppo di cooperazione NIS o della Commissione a norma dell'articolo 99, la Commissione può adottare le misure di cui agli articoli 102 e 103.

La Commissione può individuare, mediante atti di esecuzione, le risorse TIC chiave utilizzate per la fabbricazione di prodotti e la fornitura di servizi da parte dei tipi di soggetti di cui all'allegato I e all'allegato II della direttiva (UE) 2022/2555. L'articolo 102 specifica ulteriormente gli elementi da prendere in considerazione per l'individuazione delle risorse TIC chiave. L'articolo 103 stabilisce possibili misure di attenuazione nella catena di approvvigionamento delle TIC. La Commissione può decidere, mediante atti di esecuzione, di imporre nei confronti dei soggetti che operano in settori ad alta criticità e in altri settori critici misure di attenuazione specifiche, ulteriormente specificate nell'articolo.

Dopo aver effettuato una valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo, la Commissione, mediante atti di esecuzione, stila elenchi di fornitori ad alto rischio pertinenti per i divieti stabiliti negli atti di esecuzione adottati a norma dell'articolo 103, paragrafi 1 e 7, o per il divieto di cui all'articolo 110, paragrafo 1. Essa dovrebbe consultare i fornitori interessati e le autorità competenti (articolo 104).

Un soggetto stabilito in un paese terzo che desta preoccupazioni per la cibersecurity o controllato da soggetti di un tale paese terzo designato a norma dell'articolo 100 può chiedere di essere autorizzato a fornire componenti TIC destinati a risorse TIC chiave di soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 e a partecipare agli appalti pubblici in relazione alla fornitura di tali componenti TIC. L'articolo 105 specifica cosa dovrebbe contenere la richiesta e qual è la procedura per tale esenzione. L'articolo 106 specifica i diritti della difesa del soggetto in questione. La Commissione tiene un registro accessibile al pubblico delle decisioni relative alle esenzioni (articolo 107). Gli articoli 108 e 109 specificano le norme in materia di riservatezza e i diritti relativi alla procedura di esenzione.

Il capo II prevede l'applicazione del quadro per catene di approvvigionamento delle TIC affidabili alle reti di comunicazione elettronica mobili, fisse e satellitari, garantendo l'allineamento all'atto legislativo sulle reti digitali.

Le risorse TIC chiave per le reti di comunicazione elettronica mobili, fisse e satellitari figurano nell'allegato II. Il periodo di transizione per l'eliminazione graduale dei componenti TIC di fornitori ad alto rischio per le risorse TIC chiave della rete di comunicazione elettronica mobile non supera i 36 mesi dall'entrata in vigore del presente regolamento. I periodi transitori per le reti di comunicazione elettronica fisse e satellitari sono specificati dalla Commissione mediante atti di esecuzione. Alla Commissione è conferito il potere di adottare atti delegati per modificare le risorse TIC chiave designate e i periodi transitori, anche per le future generazioni di reti mobili (articolo 110). L'articolo 111 stabilisce che i fornitori di reti di comunicazione elettronica mobili, fisse e satellitari non possono utilizzare, installare o integrare, in alcuna forma, componenti TIC di fornitori ad alto rischio e non possono ottenere un'autorizzazione generale o individuale.

Autorità competenti, vigilanza ed esecuzione, giurisdizione, diritti della difesa (capo III)

Il capo III stabilisce norme dettagliate in materia di autorità competenti, vigilanza, esecuzione e giurisdizione.

Gli articoli da 112 a 114 specificano i poteri, i mezzi e le responsabilità degli Stati membri nel garantire l'attuazione e l'applicazione delle disposizioni del titolo IV. Gli Stati membri devono designare una o più autorità competenti, da notificare alla Commissione. L'articolo 113 prevede che la Commissione istituisca una rete di cooperazione tra le autorità competenti degli Stati membri e la Commissione per facilitare la conformità, mentre l'articolo 114 specifica le misure di vigilanza e di esecuzione che le autorità competenti sono autorizzate ad

adottare. Le sanzioni in caso di violazione delle disposizioni del titolo IV sono specificate all'articolo 115. L'articolo 116 contiene disposizioni dettagliate in merito alla possibilità per gli Stati membri di assistersi reciprocamente quando i soggetti svolgono attività transfrontaliere o quando le loro risorse TIC chiave sono situate in più Stati membri. L'articolo 117 stabilisce le norme in materia di competenza giurisdizionale e territorialità.

TITOLO VI: DISPOSIZIONI FINALI

Il titolo VI del regolamento proposto comprende le disposizioni finali, che delineano le norme riguardanti l'adozione di atti delegati e di esecuzione, il processo di valutazione della proposta di regolamento e l'abrogazione e sostituzione del regolamento (UE) 2019/881. Fissa inoltre la data di entrata in vigore del regolamento proposto.

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,
visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,
vista la proposta della Commissione europea,
previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,
visto il parere del Comitato economico e sociale europeo²⁴,
visto il parere del Comitato delle regioni²⁵,
deliberando secondo la procedura legislativa ordinaria,
considerando quanto segue:

- (1) Dall'adozione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio²⁶, il panorama geopolitico, tecnologico e delle politiche ha subito trasformazioni significative. Gli incidenti di cibersicurezza, causati da guasti del sistema, errori umani, atti dolosi o fenomeni naturali sono aumentati, e gli attacchi informatici sono diventati più sofisticati, colpendo soggetti essenziali, imprese e il pubblico in generale. L'ecosistema della criminalità informatica, e in particolare l'attività di ransomware, ha registrato una crescita vertiginosa. Gli incidenti nella catena di approvvigionamento, sia che siano causati da criminali a scopo di lucro o da soggetti statali a fini di perturbazione, spionaggio, disinformazione o guerra, si sono intensificati. Nell'ambito di una più ampia strategia ibrida, gli incidenti derivanti da attività informatiche dolose e guasti del sistema si propagano a macchia d'olio, perturbando i servizi essenziali, minando la fiducia nelle istituzioni e compromettendo la preparazione sociale e la preparazione alla difesa dell'Unione. Tali incidenti hanno dimostrato di poter incidere sull'attività economica, sulla stabilità finanziaria e sulla vita delle persone. Allo stesso tempo, la vulnerabilità delle infrastrutture e dei sistemi

²⁴ GU C [...] del [...], pag. [...].

²⁵ GU C [...] del [...], pag. [...].

²⁶ 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, ELI: <http://data.europa.eu/eli/reg/2019/881/oj>).

civili critici rappresenta un rischio per le capacità di difesa che fanno affidamento su di essi.

- (2) Nel contempo, tecnologie emergenti come l'intelligenza artificiale e l'informatica quantistica stanno avendo un effetto dirompente sulla cibersicurezza e sulla ciberdifesa. Queste tecnologie stanno ridefinendo gli strumenti di difesa e le tattiche degli avversari e rappresentano una minaccia per la cibersicurezza e la ciberdifesa, offrendo però al contempo possibilità di progresso tecnologico. Sebbene possano contribuire alla cibersicurezza attraverso un migliore rilevamento delle minacce o una risposta automatizzata agli incidenti, queste tecnologie stanno anche offrendo alle organizzazioni criminali una più ampia superficie complessiva di attacco, sono potenziali bersagli di manipolazione e possono compromettere l'efficacia a lungo termine di misure di sicurezza quali la crittografia.
- (3) Per far fronte a tali sviluppi, l'Unione ha rafforzato i suoi strumenti giuridici e politici. La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio²⁷ rafforza la cibersicurezza delle infrastrutture critiche, integrata dalla direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio²⁸ per quanto concerne la sicurezza fisica. Il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio²⁹ rafforza la cibersicurezza dei prodotti con elementi digitali. Il regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio³⁰ crea capacità di risposta a livello dell'Unione, e la raccomandazione del Consiglio, del 6 giugno 2025, relativa a un programma dell'UE per la gestione delle crisi informatiche³¹ ("raccomandazione relativa al programma per la cibersicurezza") sostiene la cooperazione a livello dell'Unione in materia di gestione delle crisi. Il pacchetto di strumenti per la cibersicurezza del 5G³² costituisce un primo passo verso un approccio coordinato a livello dell'Unione per garantire la sicurezza delle reti 5G. La comunicazione della Commissione sull'Accademia per le competenze in materia di cibersicurezza³³ affronta la crescente sfida del divario di talenti nel settore della cibersicurezza. Il quadro per la cibersicurezza è stato inoltre rafforzato dalla normativa settoriale, in particolare dal

²⁷ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

²⁸ Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (GU L 333 del 27.12.2022, pag. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>).

²⁹ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

³⁰ Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (GU L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>).

³¹ GU C, C/2025/3445, 20.6.2025, ELI: <http://data.europa.eu/eli/C/2025/3445/oj>.

³² Gruppo di cooperazione NIS, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, 1/2020, disponibile all'indirizzo: <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

³³ Comunicazione della Commissione al Parlamento europeo e al Consiglio, Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza") (COM(2023) 207 final del 18 aprile 2023).

regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio³⁴ per il settore finanziario, dal regolamento delegato (UE) 2024/1366 della Commissione³⁵ per il sottosettore dell'energia elettrica, dal regolamento delegato (UE) 2022/1645 della Commissione³⁶ e dal regolamento di esecuzione (UE) 2023/203 della Commissione³⁷ (parte IS), nonché dalle pertinenti norme in materia di sicurezza aerea di cui al regolamento (UE) 2019/1583 della Commissione³⁸ per il sottosettore del trasporto aereo, e da altri documenti strategici quali la comunicazione della Commissione relativa a un piano d'azione dell'UE sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria³⁹. I soggetti dell'Unione sono inoltre rafforzati dal regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio⁴⁰, che stabilisce misure volte a conseguire un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione. Nell'ambito di tale quadro giuridico rafforzato per la cibersicurezza sono stati ulteriormente specificati i compiti dell'ENISA.

³⁴ Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>).

³⁵ Regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio istituendo un codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica (GU L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

³⁶ Regolamento delegato (UE) 2022/1645 della Commissione, del 14 luglio 2022, recante modalità di applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le imprese disciplinate dai regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione e che modifica i regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione (GU L 248 del 26.9.2022, pag. 18, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

³⁷ Regolamento di esecuzione (UE) 2023/203 della Commissione, del 27 ottobre 2022, che stabilisce le regole per l'applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti relativi alla gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le organizzazioni di cui ai regolamenti (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011 e (UE) 2015/340 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e per le autorità competenti di cui ai regolamenti (UE) n. 748/2012, (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011, (UE) 2015/340 e (UE) n. 139/2014 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e che modifica i regolamenti (UE) n. 1178/2011, (UE) n. 748/2012, (UE) n. 965/2012, (UE) n. 139/2014, (UE) n. 1321/2014 e (UE) 2015/340 della Commissione e i regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione (GU L 31 del 2.2.2023, pag. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

³⁸ Regolamento di esecuzione (UE) 2019/1583 della Commissione, del 25 settembre 2019, che modifica il regolamento di esecuzione (UE) 2015/1998 che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, per quanto riguarda le misure di cibersicurezza (GU L 246 del 26.9.2019, pag. 15, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

³⁹ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria (COM(2025) 10 final del 15 gennaio 2025).

⁴⁰ 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 (GU L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>).

- (4) In tale contesto, e come affermato nel documento "ProtectEU: strategia europea di sicurezza interna"⁴¹, e nella strategia per l'Unione della preparazione⁴², per garantire la preparazione, la sicurezza e la resilienza della società e dell'economia dell'Unione sono necessari un forte coordinamento, fiducia e condivisione delle informazioni a livello europeo tra i portatori di interessi, quadri solidi volti a garantire la sicurezza dei prodotti, dei servizi, dei processi TIC e dei servizi di sicurezza gestiti, come pure la crescita e il rafforzamento della forza lavoro nel settore della cibersecurity. In tale documento si invita inoltre a rafforzare le catene di approvvigionamento delle TIC garantendo la sovranità tecnologica europea sulle risorse chiave, il che aumenterebbe la resilienza dell'Unione e potrebbe giovare agli sforzi di ciberdifesa. Inoltre la comunicazione sul rafforzamento della sicurezza economica dell'UE⁴³ individua come obiettivi prioritari la necessità di impedire l'accesso a informazioni e dati sensibili che potrebbero compromettere la sicurezza economica dell'UE e di prevenire e attenuare le perturbazioni delle infrastrutture critiche dell'UE che incidono sulla sua economia. Nella comunicazione si riconosce il ruolo essenziale svolto a tale riguardo da misure efficaci in materia di cibersecurity.
- (5) Gli incidenti di cibersecurity su vasta scala che colpiscono infrastrutture critiche, servizi digitali o funzioni sociali essenziali possono avere ripercussioni sulla popolazione che richiedono un'azione coordinata di protezione civile e di gestione delle crisi a livello dell'Unione. In linea con l'approccio multirischio della strategia europea per l'Unione della preparazione e della decisione n. 1313/2013/UE su un meccanismo unionale di protezione civile, le disposizioni in materia di conoscenza situazionale, risposta agli incidenti ed esercitazioni a norma del presente regolamento dovrebbero confluire nella gestione delle crisi dell'Unione, in particolare attraverso il Centro di coordinamento della risposta alle emergenze (*Emergency Response Coordination Centre* – ERCC).
- (6) La presente proposta è coerente con la [proposta di direttiva che integra [la revisione del regolamento (UE) 2019/881] e modifica la direttiva (UE) 2022/2555 per quanto riguarda la semplificazione dell'attuazione di misure per un livello comune elevato di cibersecurity nell'Unione], che la integra, nonché con la [proposta di regolamento sulla semplificazione della legislazione sul digitale (omnibus digitale)]⁴⁴ che prevede l'obbligo per l'ENISA di istituire un punto di accesso unico per la segnalazione degli incidenti attraverso il quale i soggetti possano adempiere contemporaneamente agli obblighi di segnalazione degli incidenti previsti da molteplici atti giuridici.
- (7) Il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio⁴⁵ ha istituito l'ENISA con l'obiettivo di contribuire ad assicurare un livello di sicurezza elevato ed efficace delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una

⁴¹ Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, ProtectEU: strategia europea di sicurezza interna (COM(2025) 148 final del 1° aprile 2025).

⁴² Comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia europea per l'Unione della preparazione (JOIN(2025) 130 final).

⁴³ Comunicazione congiunta al Parlamento europeo e al Consiglio, Rafforzare la sicurezza economica dell'UE (JOIN(2025) 977 final).

⁴⁴ [COM\(2025\) 837 final](#).

⁴⁵ Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1, ELI: <http://data.europa.eu/eli/reg/2004/460/oj>).

cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni pubbliche. Il mandato dell'ENISA è stato prorogato tre volte prima che il regolamento (UE) 2019/881 le conferisse un mandato permanente. Al fine di rispondere meglio alle esigenze generate dall'evoluzione del panorama delle minacce e della tecnologia, in particolare per quanto riguarda la cooperazione operativa e la crescente necessità di professionisti della cibersicurezza, il mandato dell'ENISA dovrebbe essere ulteriormente rafforzato. Ai fini della certezza del diritto è opportuno sostituire il regolamento (UE) 2019/881.

- (8) In un contesto caratterizzato da minacce in continua evoluzione, in cui gli incidenti di cibersicurezza diventano sempre più significativi, è più importante che mai rafforzare la fiducia dei cittadini, delle autorità pubbliche e delle imprese nell'uso quotidiano delle tecnologie. Un aumento della fiducia può essere agevolato da un rafforzamento del quadro europeo di certificazione della cibersicurezza a livello di Unione che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali. Il nuovo quadro dovrebbe stabilire i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza e consentire il riconoscimento e l'utilizzo dei certificati europei di cibersicurezza e delle dichiarazioni UE di conformità in tutti gli Stati membri. A tal fine, dovrebbe istituire una procedura e un quadro di governance che consentano lo sviluppo e il mantenimento tempestivi e prevedibili di sistemi europei di certificazione della cibersicurezza. I sistemi europei di certificazione della cibersicurezza dovrebbero essere applicati in modo uniforme in tutti gli Stati membri per garantire un'attuazione armonizzata dei requisiti di cibersicurezza, creare condizioni di parità e prevenire la scelta opportunistica della certificazione più vantaggiosa in base ai diversi livelli di rigore nei vari Stati membri. L'ENISA dovrebbe svolgere un ruolo fondamentale nel garantire lo sviluppo dei sistemi mediante specifiche tecniche e nell'assicurare che tali sistemi rimangano aggiornati dal punto di vista tecnico. Inoltre, per rispondere in modo efficace alle esigenze del mercato, il quadro dovrebbe prevedere la possibilità di certificare le misure di gestione dei rischi di cibersicurezza rivolte ai soggetti e facilitare il rispetto di altre normative dell'Unione applicabili nel settore della cibersicurezza. L'allineamento al diritto dell'Unione vigente, come il regolamento (UE) 2024/2847 e la direttiva (UE) 2022/2555, è essenziale affinché i sistemi europei di certificazione della cibersicurezza contribuiscano a ridurre gli oneri di conformità che gravano sulle imprese, rendendole più attraenti, e a rafforzare la ciberresilienza dell'Unione.
- (9) La missione dell'ENISA dovrebbe essere quella di sostenere gli Stati membri e i soggetti dell'Unione nel conseguimento di un livello elevato di cibersicurezza, di resilienza e di fiducia all'interno dell'Unione. A tal fine, l'ENISA dovrebbe fungere da punto di riferimento per consulenze e competenze in materia di cibersicurezza e il suo operato dovrebbe ruotare principalmente intorno a quattro ambiti chiave della cibersicurezza a livello dell'Unione. In primo luogo, l'ENISA dovrebbe sostenere gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza e assisterli attraverso attività di sviluppo delle capacità volte al costante miglioramento delle loro capacità in termini di preparazione, resilienza e risposta. In secondo luogo, l'ENISA dovrebbe contribuire alla cooperazione operativa a livello dell'Unione, tra gli Stati membri, e a una maggiore condivisione della conoscenza situazionale in merito alle minacce e agli incidenti informatici tra gli Stati membri e i soggetti dell'Unione. Il terzo ambito chiave dovrebbe essere la certificazione della cibersicurezza e la normazione, mentre il quarto dovrebbe essere la realizzazione dell'Accademia per le competenze in materia di cibersicurezza, che

dovrebbe contribuire allo sviluppo di una forza lavoro europea dinamica nel settore della cibersicurezza con competenze che dovrebbero essere trasferibili in tutti gli Stati membri.

- (10) Il regolamento (UE, Euratom) 2023/2841 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione e conferisce al CERT-UE, rinominato servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione, il mandato di contribuire alla sicurezza dell'ambiente TIC non riservato dei soggetti dell'Unione fornendo loro consulenza in materia di cibersicurezza, aiutandoli a prevenire, rilevare, affrontare e attenuare gli incidenti, nonché a rispondervi e riprendersi dagli stessi, e fungendo per tali soggetti da piattaforma per lo scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti. Inoltre il CERT-UE ha il compito di offrire i pertinenti servizi di cibersicurezza ai soggetti dell'Unione. Nell'ambito della sua missione, l'ENISA dovrebbe sostenere anche i soggetti dell'Unione. In particolare, dovrebbe assolvere tale compito avviando una cooperazione strutturata con il CERT-UE in materia di sviluppo delle capacità, cooperazione operativa e analisi strategiche a lungo termine delle minacce informatiche. Se del caso, l'ENISA può avvalersi della cooperazione strutturata con il CERT-UE per offrire servizi o sostegno in materia di cibersicurezza che possono apportare un valore aggiunto ai soggetti dell'Unione, in modo coordinato al fine di garantire sinergie con l'operato del CERT-UE.
- (11) Uno dei compiti fondamentali dell'ENISA dovrebbe essere quello di fornire sostegno agli Stati membri nell'attuazione coerente delle politiche e del diritto dell'Unione in materia di cibersicurezza, in particolare per quanto riguarda la direttiva (UE) 2022/2555, il regolamento (UE) 2024/2847 e il regolamento (UE) 2025/38. Per facilitare un'attuazione coerente ed efficace dell'*acquis* dell'Unione in materia di cibersicurezza, l'ENISA dovrebbe pubblicare orientamenti tecnici e relazioni, fornire consulenza e migliori pratiche e agevolare lo scambio di migliori pratiche tra le autorità competenti a tal fine. L'ENISA valuta costantemente lo stato della cibersicurezza nell'Unione e a tal fine adotta una relazione conformemente all'articolo 18 della direttiva (UE) 2022/2555. L'ENISA dovrebbe inoltre essere in grado di rispondere alle richieste di consulenza e assistenza da parte degli Stati membri e, se del caso, dei soggetti dell'Unione, su materie che rientrano nel suo mandato.
- (12) Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, in particolare per sostenere la protezione delle infrastrutture critiche, l'ENISA dovrebbe sostenere la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano negli allegati I e II della direttiva (UE) 2022/2555, e delle informazioni relative ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847. Tale sostegno può consistere nel fornire migliori pratiche e orientamenti sugli strumenti disponibili e sulle procedure, nonché nel fornire orientamenti su come affrontare le questioni normative relative alla condivisione delle informazioni, ad esempio agevolando la creazione di centri settoriali di condivisione e analisi delle informazioni.
- (13) Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni, l'ENISA dovrebbe contribuire ai lavori del gruppo di cooperazione istituito dalla direttiva (UE) 2022/2555 ("gruppo di cooperazione NIS"), in particolare mettendo a disposizione competenze, fornendo consulenze e agevolando lo scambio di migliori pratiche, tra l'altro in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti. L'ENISA dovrebbe inoltre contribuire ai lavori del gruppo di cooperazione per l'identità digitale europea istituito dal regolamento (UE) n. 910/2014

del Parlamento europeo e del Consiglio⁴⁶, del gruppo europeo per la certificazione della cibersicurezza e del gruppo di cooperazione amministrativa (ADCO) istituito dal regolamento (UE) 2024/2847.

- (14) Il nucleo pubblico di una rete internet aperta, vale a dire i suoi protocolli e le sue infrastrutture principali, che costituiscono un bene pubblico globale, consente la funzionalità essenziale di internet nel suo complesso e ne supporta il normale funzionamento. Nell'ambito del suo mandato, l'ENISA dovrebbe sostenere la sicurezza e la resilienza del nucleo pubblico della rete internet aperta e la stabilità del suo funzionamento, compresi, solo a titolo di esempio, la diffusione e il funzionamento sicuri dei protocolli chiave (in particolare il sistema dei nomi di dominio, il protocollo di instradamento BGP (*Border Gateway Protocol*) e il protocollo Internet versione 6) e il funzionamento del sistema dei nomi di dominio (come il funzionamento di tutti i domini di primo livello), attraverso la promozione di migliori pratiche, orientamenti e cooperazione, conformemente alle disposizioni consolidate in materia di governance globale e multipartecipativa di internet e ai rispettivi ruoli e responsabilità degli organismi tecnici e operativi internazionali competenti.
- (15) L'ENISA funge da punto di riferimento per consulenza e competenze in materia di cibersicurezza. Pertanto, su richiesta della Commissione, l'ENISA dovrebbe fornire assistenza mediante competenze, consulenza tecnica, informazioni, analisi, compresi studi di fattibilità, pareri e lavori preparatori su ogni aspetto specifico del settore della cibersicurezza, al fine di orientare l'elaborazione delle politiche della Commissione e facilitare il monitoraggio da parte di quest'ultima dell'attuazione della legislazione dell'Unione in materia di cibersicurezza.
- (16) Analogamente, tenendo conto delle sue competenze, l'ENISA dovrebbe assistere gli Stati membri nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare le minacce e gli incidenti e relativi alla sicurezza dei sistemi informativi e di rete e per reagirvi. In particolare, l'ENISA dovrebbe sostenere lo sviluppo e il potenziamento dei gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Teams* – "CSIRT") previsti dalla direttiva (UE) 2022/2555 perché raggiungano un livello comune elevato di maturità nell'Unione.
- (17) L'ENISA ha sostenuto e dovrebbe continuare a sostenere gli Stati membri nell'elaborazione e nell'attuazione di orientamenti per le rispettive strategie nazionali per la cibersicurezza contribuendo all'adozione e all'attuazione di tali strategie da parte di tutti gli Stati membri. L'ENISA dovrebbe promuovere la diffusione di tali strategie attraverso la mappa interattiva delle strategie nazionali per la cibersicurezza e dovrebbe seguire ulteriormente i progressi compiuti nella loro attuazione, anche fornendo sostegno nello sviluppo di indicatori chiave di prestazione in tale contesto.
- (18) Il regolamento (UE, Euratom) 2023/2841 ha incaricato il comitato interistituzionale per la cibersicurezza di sostenere i soggetti dell'Unione nell'incrementare le rispettive posture di cibersicurezza e il CERT-UE di contribuire alla sicurezza dell'ambiente TIC non riservato di tutti i soggetti dell'Unione. L'ENISA, sulla base della sua esperienza in materia di cibersicurezza, dovrebbe sostenere il comitato interistituzionale per la

⁴⁶ Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

cibersicurezza e il CERT-UE nei loro compiti di cui al regolamento (UE, Euratom) 2023/2841, anche contribuendo all'analisi delle minacce informatiche, alla conoscenza situazionale informatica, alle esercitazioni di cibersicurezza, al coordinamento della risposta agli incidenti e allo scambio di conoscenze e migliori pratiche.

- (19) Sulla base delle proprie competenze e per integrare le capacità delle autorità pubbliche nazionali e dell'Unione, l'ENISA dovrebbe offrire programmi di formazione utilizzando come base il quadro europeo delle competenze in materia di cibersicurezza (*European Cybersecurity Skills Framework – ECSF*), in particolare per sostenere l'attuazione efficace delle politiche, la cooperazione operativa e le attività di sensibilizzazione.
- (20) Per garantire sinergie con il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e con la rete dei centri nazionali di coordinamento istituiti a norma del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio⁴⁷, l'ENISA dovrebbe sostenerli condividendo informazioni sui rischi e sulle minacce informatiche attuali ed emergenti, compresi i rischi e le minacce relativi alle tecnologie dell'informazione e della comunicazione.
- (21) La strategia per la preparazione sottolinea che l'alfabetizzazione digitale, che si basa sull'acquisizione di competenze digitali di base, è essenziale per l'emancipazione di cittadini più resilienti di fronte a potenziali crisi. Tuttavia, come sottolineato nella comunicazione della Commissione sull'Unione delle competenze⁴⁸, quasi la metà della popolazione adulta non dispone delle competenze digitali di base, nonostante oltre il 90 % dei posti di lavoro le richieda. Al fine di garantire che la forza lavoro attuale e potenziale futura disponga delle competenze necessarie in un ambiente digitale in rapida evoluzione e di contribuire allo sviluppo della riserva di talenti europei in materia di cibersicurezza, l'ENISA dovrebbe sostenere attività di sensibilizzazione in materia di cibersicurezza, come la European Cybersecurity Challenge, volte ad attrarre talenti e a contribuire a informare in merito all'istruzione e alle competenze necessarie nel settore della cibersicurezza. A tale riguardo, l'ENISA dovrebbe coordinare competizioni in materia di cibersicurezza, eventi "Capture the Flag" e simili esercitazioni pratiche, quale mezzo per sviluppare le competenze in materia di cibersicurezza e promuovere lo sviluppo di capacità in tutta l'Unione. Nello svolgimento delle attività di sensibilizzazione, l'ENISA dovrebbe garantire che esse rispondano alle esigenze delle autorità pubbliche nazionali e dei soggetti dell'Unione, nonché alle esigenze delle imprese, in particolare delle PMI, e degli istituti di istruzione e formazione, mantenendo aggiornati quadri pratici e opportunità di formazione, quale ad esempio l'"awareness-raising-in-a-box". L'ENISA dovrebbe sviluppare ulteriormente orientamenti pratici e attuabili per sostenere l'attuazione della politica e della normativa dell'Unione in materia di cibersicurezza. L'ENISA dovrebbe inoltre impegnarsi a comunicare le informazioni pertinenti relative ai sistemi di certificazione applicabili, ad esempio fornendo orientamenti e raccomandazioni.

⁴⁷ Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento (GU L 202 dell'8.6.2021, pag. 1, ELI: <http://data.europa.eu/eli/reg/2021/887/oj>).

⁴⁸ Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, L'Unione delle competenze (COM(2025) 90 final del 5 marzo 2025).

- (22) Per sostenere le imprese che operano nel settore della cibersecurity e gli utenti delle soluzioni di cibersecurity e per garantire l'efficace attuazione del titolo III del presente regolamento, l'ENISA dovrebbe sviluppare e mantenere un "osservatorio del mercato" mediante l'esecuzione di analisi periodiche e la diffusione di informazioni sulle principali tendenze del mercato della cibersecurity, sul versante sia della domanda che dell'offerta. Inoltre, per sostenere gli utenti della riserva dell'UE per la cibersecurity istituita a norma del regolamento (UE) 2025/38, l'ENISA dovrebbe preparare, ai sensi del medesimo regolamento, la mappatura dei servizi necessari a tali utenti e della disponibilità di tali servizi.
- (23) Le minacce informatiche sono un problema globale. È necessaria una più stretta cooperazione internazionale per migliorare la cibersecurity, così come la definizione di norme di comportamento e di approcci comuni. A tal fine, l'ENISA dovrebbe sostenere la cooperazione dell'Unione con i paesi terzi, con particolare attenzione ai paesi candidati all'adesione all'Unione, e con le organizzazioni internazionali, come la NATO, fornendo le competenze e le analisi necessarie alla Commissione e ai pertinenti soggetti dell'Unione, se del caso. Le attività dell'ENISA nel settore internazionale dovrebbero sempre essere in linea con le priorità dell'Unione.
- (24) Per contribuire al conseguimento di un livello elevato di cibersecurity nell'Unione, l'ENISA dovrebbe sostenere la cooperazione operativa tra gli Stati membri, in cooperazione con il CERT-UE, tra i soggetti dell'Unione e tra i portatori di interessi. A tal fine, il ruolo dell'ENISA dovrebbe essere rafforzato. L'ENISA dovrebbe diventare membro della rete di CSIRT, contribuendo allo scambio di informazioni e all'attività di analisi. L'ENISA dovrebbe promuovere e sostenere ulteriormente la cooperazione tra i CSIRT interessati in caso di incidenti, attacchi o perturbazioni delle reti o delle infrastrutture della cui gestione o protezione sono responsabili i CSIRT. Il sostegno attivo dell'ENISA ai lavori della rete di CSIRT e della rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) dovrebbe consentire a tali reti di continuare a rafforzare il loro livello di maturità. Il ruolo dell'ENISA nel sostenere tale cooperazione comprende la lotta contro le minacce alla sicurezza e all'integrità delle istituzioni, delle elezioni e di altri processi democratici, nonché delle infrastrutture critiche da cui dipendono, in linea con lo scudo europeo per la democrazia a puntello di democrazie solide e resilienti⁴⁹.
- (25) Per sostenere lo sviluppo di capacità, la cooperazione operativa e le analisi strategiche a lungo termine delle minacce informatiche, l'ENISA dovrebbe avvalersi delle competenze tecniche e operative disponibili del CERT-UE attraverso una cooperazione strutturata, ad esempio mediante appositi accordi.
- (26) Al fine di rafforzare la cibersecurity in tutta l'Unione e garantire una risposta rapida ed efficace alle minacce informatiche, l'ENISA dovrebbe sostenere gli Stati membri, su loro richiesta, anche fornendo consulenza sul miglioramento delle loro capacità di prevenire e rilevare gli incidenti, nonché di rispondervi e riprendersi dagli stessi, agevolando la gestione tecnica degli incidenti significativi ai sensi della direttiva (UE) 2022/2555, in particolare sostenendo la condivisione volontaria di soluzioni tecniche tra gli Stati membri o assicurando che minacce e incidenti informatici siano analizzati. L'ENISA dovrebbe inoltre assistere EU-CyCLONe nella preparazione di relazioni a livello politico dell'Unione e degli Stati membri.

⁴⁹ JOIN(2025) 791 final.

- (27) Per ridurre l'esposizione alle ingerenze straniere, alla manipolazione della catena di approvvigionamento e all'esfiltrazione di dati strategici, l'ENISA dovrebbe utilizzare strumenti di comunicazione sicura nell'ambito della rete di CSIRT e di EU-CyCLONe. In base alla raccomandazione relativa al programma per la cibersecurity, tali strumenti dovrebbero essere forniti da soggetti giuridici stabiliti o considerati stabiliti negli Stati membri e controllati da Stati membri o da cittadini degli Stati membri.
- (28) Per contribuire alla preparazione e alla risposta a livello dell'Unione in caso di crisi e incidenti di cibersecurity su vasta scala, l'ENISA dovrebbe svolgere attività volte alla conoscenza situazionale in materia di cibersecurity.
- (29) L'accesso all'intelligence in tempo reale, verificata e affidabile sulle minacce informatiche è fondamentale per costruire una conoscenza situazionale condivisa nell'Unione. L'ENISA, la Commissione, il CERT-UE e il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol hanno già sviluppato archivi di intelligence sulle minacce informatiche adattati alle proprie esigenze specifiche. L'ENISA e altri soggetti pertinenti dell'Unione dovrebbero cooperare, su base volontaria, per sviluppare archivi di dati sulle minacce informatiche in tempo reale, verificati e affidabili e cercare di creare sinergie per assicurare economie di scala e una più sana gestione finanziaria. Dovrebbero operare in tal senso anche soggetti settoriali dell'Unione quali l'agenzia dell'Unione europea per il programma spaziale. Tali soggetti dovrebbero condividere soltanto analisi, tendenze e tattiche, tecniche e procedure derivate, non fonti grezze, e dovrebbe essere rispettata la loro indipendenza per quanto riguarda la gestione del ciclo di vita dei dati sulle minacce informatiche in linea con i rispettivi mandati e le rispettive norme in materia di "necessità di conoscere".
- (30) Al fine di contribuire a una risposta tempestiva e coordinata, l'ENISA dovrebbe poter trasmettere allerte precoci in caso di incidente significativo o su vasta scala, potenziale o in corso, o di minaccia informatica di potenziale natura transfrontaliera al CSIRT o ai CSIRT interessati e, se del caso, alla rete di CSIRT e a EU-CyCLONe, in particolare in relazione ai soggetti elencati negli allegati I e II della direttiva (UE) 2022/2555. Le informazioni contenute in tali allerte precoci possono includere vulnerabilità pubblicamente note e l'eventuale compromissione di prodotti con elementi digitali di cui al regolamento (UE) 2024/2847, nonché tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce e raccomandazioni sulle misure di attenuazione.
- (31) Al fine di preservare la fiducia e non compromettere la condivisione delle informazioni, è importante che l'ENISA applichi contrassegni visibili che indichino in che misura un documento o un'informazione da essa prodotti o ricevuti possano essere ulteriormente condivisi. Analogamente, l'ENISA dovrebbe utilizzare i documenti o le informazioni che riceve per lo svolgimento delle proprie attività, fatte salve eventuali limitazioni all'ulteriore distribuzione di tali informazioni mediante un contrassegno visibile.
- (32) Per contribuire ad accrescere la consapevolezza in merito agli indicatori delle minacce informatiche e alle raccomandazioni sulle misure di attenuazione, l'ENISA dovrebbe mettere a disposizione dei soggetti che operano nei settori elencati negli allegati I e II della direttiva (UE) 2022/2555 un servizio di allerta precoce. Tali allerte precoci, di carattere generico e di tipo volontario, dovrebbero andare soprattutto a vantaggio delle PMI e dovrebbero essere fornite in un formato pubblicamente disponibile e leggibile da un dispositivo automatico. In ogni caso, tale servizio volontario è distinto da

eventuali partenariati pubblico-privato che l'ENISA abbia già istituito o potrebbe istituire e non ha con essi alcun collegamento.

- (33) Al fine di sostenere la conoscenza situazionale condivisa, l'ENISA dovrebbe elaborare periodicamente, in stretta cooperazione con gli Stati membri, una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatiche, sulla base di informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise dai CSIRT degli Stati membri o dai punti di contatto unici in materia di sicurezza dei sistemi informativi e di rete ("punti di contatto unici") previsti dalla direttiva (UE) 2022/2555, in entrambi i casi su base volontaria, da Europol e dal CERT-UE. Tale relazione dovrebbe essere messa a disposizione del Consiglio, del servizio europeo per l'azione esterna, di EU-CyCLONe, della rete di CSIRT, della Commissione e di Europol.
- (34) Al fine di migliorare la conoscenza situazionale condivisa del panorama delle minacce e degli incidenti informatici tra i portatori di interessi, l'ENISA dovrebbe analizzare le tendenze in materia di minacce e incidenti informatici. Ciò dovrebbe includere un'analisi periodica riguardante i settori ad alta criticità e altri settori critici elencati negli allegati I e II della direttiva (UE) 2022/2555, compresi i settori dell'assistenza sanitaria, dell'energia e dei trasporti. L'analisi dovrebbe riguardare anche i livelli di maturità dei settori e individuare, tra l'altro, le possibili sfide specifiche di un determinato settore. Se del caso, e al fine di individuare gli effetti sulla catena di approvvigionamento, l'analisi dovrebbe dimostrare le minacce informatiche e le tendenze relative alle categorie di prodotti contemplate dal regolamento (UE) 2024/2847. L'ENISA dovrebbe sviluppare competenze nel settore della cibersicurezza delle infrastrutture e delle relative dipendenze nelle catene di approvvigionamento critiche, in particolare per sostenere i settori elencati negli allegati I e II della direttiva (UE) 2022/2555 e l'attuazione del regolamento (UE) 2024/2847. A tal fine, l'ENISA dovrebbe anche cooperare, se del caso, con altri soggetti pertinenti dell'Unione.
- (35) Inoltre, per comprendere meglio le sfide nel campo della cibersicurezza, l'ENISA deve analizzare le tecnologie attuali ed emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti, dal punto di vista sociale, giuridico, economico e regolamentare, delle innovazioni tecnologiche sulla cibersicurezza. Al fine di agevolare l'accesso del pubblico a informazioni sui rischi di cibersicurezza e sulle possibili soluzioni, l'ENISA può fornire informazioni pertinenti sul suo sito web, in modo facilmente fruibile e ben strutturato.
- (36) Il rafforzamento del ruolo dell'ENISA nella promozione della conoscenza situazionale, nell'analisi delle minacce e nella fornitura di consulenza tecnica contribuirà a dare maggior vigore agli sforzi collettivi in materia di cibersicurezza per quanto riguarda i prodotti con elementi digitali e sosterrà l'attuazione del regolamento (UE) 2024/2847. Conformemente al regolamento (UE) 2024/2847, l'ENISA può proporre alle autorità di vigilanza del mercato attività congiunte volte a verificare la conformità dei prodotti con elementi digitali e individuare le categorie di prodotti con elementi digitali per le quali possono essere organizzate indagini a tappeto. Le informazioni risultanti dall'analisi delle minacce informatiche e delle allerte precoci dovrebbero rafforzare il sostegno che l'ENISA fornisce a tali autorità e contribuire a un'applicazione efficace del regolamento (UE) 2024/2847 per prevenire gli effetti degli attacchi informatici sulle catene di approvvigionamento in tutto il mercato interno e migliorare la preparazione generale dell'Unione.

- (37) Gli attacchi ransomware rappresentano una grave minaccia per la cibersecurity dell'Unione. Per rafforzare la cibersecurity dell'Unione e lottare contro il fenomeno dei ransomware, l'ENISA dovrebbe sviluppare capacità di conoscenza situazionale e sostegno per la risposta e la ripresa in caso di incidenti. Nell'assistere singoli soggetti essenziali e importanti a rispondere a un attacco di ransomware e a riprendersi da esso, l'ENISA dovrebbe cooperare strettamente con Europol e con i CSIRT o con le autorità competenti, a seconda dei casi, attingendo in tal modo all'esperienza consolidata di Europol nella lotta ai reati di ransomware. Tale assistenza dovrebbe integrare le attività dei CSIRT a sostegno della risposta agli incidenti. Per creare sinergie nella sua attività di lotta contro i ransomware, l'ENISA dovrebbe istituire un helpdesk e, a tal fine, potrebbe mettere in comune le capacità pertinenti e i servizi di contrasto al ransomware e rendere facilmente accessibili informazioni, orientamenti e strumenti che possano aiutare i soggetti essenziali e importanti a rispondere a un incidente di ransomware e a riprendersi da esso.
- (38) L'ENISA dovrebbe fornire competenze tecniche e sostegno alla Commissione nella preparazione di un programma continuo annuale di esercitazioni di cibersecurity a livello dell'Unione conformemente alla raccomandazione relativa al programma per prepararsi alle crisi informatiche, al fine di verificare il livello di cibersecurity dei soggetti che partecipano a tali esercitazioni, e ridurre al minimo la duplicazione degli sforzi. L'ENISA dovrebbe, ad esempio, fornire consulenza sui tipi appropriati di esercitazione, come le esercitazioni a tavolino, ibride o dal vivo, nonché sugli obiettivi, gli scenari e la partecipazione.
- (39) L'accesso a informazioni corrette e tempestive sulle vulnerabilità e una solida gestione delle vulnerabilità sono fondamentali per garantire un livello elevato di cibersecurity nel mercato interno. Per tale motivo l'ENISA dovrebbe mantenere una banca dati europea delle vulnerabilità a norma della direttiva (UE) 2022/2555 e creare una capacità comune di servizi di gestione delle vulnerabilità dell'Unione, garantendo un livello di servizio resiliente e sostenibile e riducendo il rischio di perturbazioni. A tal fine, l'ENISA dovrebbe esaminare le possibilità di approfondire la cooperazione strutturata con programmi, registri o banche dati simili alla banca dati europea delle vulnerabilità, al fine di evitare una duplicazione degli sforzi e di perseguire la complementarità a livello internazionale, ove opportuno. Inoltre l'ENISA dovrebbe sostenere la divulgazione multilaterale coordinata delle vulnerabilità a livello dell'Unione e fornire servizi a valore aggiunto, quali consigli sulle vulnerabilità, indici di gravità ed elenchi di prodotti, nonché fornire un catalogo europeo migliorato delle vulnerabilità sfruttate note per aiutare i soggetti nella gestione delle vulnerabilità.
- (40) Il ruolo dell'ENISA nello sviluppo del quadro europeo di certificazione della cibersecurity dovrebbe rappresentare un aspetto fondamentale del suo mandato. L'ENISA dovrebbe fornire le proprie competenze tecniche ai sistemi europei di certificazione della cibersecurity per l'intera durata del loro ciclo di vita. In vista di un sistema futuro, l'ENISA dovrebbe individuare le possibili norme o specifiche tecniche su cui basare tale sistema e, se del caso, elaborare essa stessa le specifiche tecniche da poter richiamare in un sistema. L'ENISA dovrebbe essere incaricata di preparare una proposta di sistema a seguito di una richiesta della Commissione. Quanto ai sistemi già esistenti, l'ENISA dovrebbe essere responsabile del loro mantenimento. A tal fine, l'ENISA dovrebbe contribuire alla creazione e allo sviluppo di un ecosistema di certificazione in cui sia richiesto il riscontro degli Stati membri e dei portatori di interessi privati e siano rafforzate le loro capacità di certificazione. Ciò dovrebbe includere anche la gestione di un apposito sito web sulla certificazione in cui

le informazioni pertinenti relative ai sistemi adottati, compresi i certificati e le dichiarazioni di conformità, siano liberamente e pubblicamente accessibili.

- (41) Per sostenere l'attuazione della pertinente normativa dell'Unione, l'ENISA dovrebbe definire lo stato dell'arte in materia di cibersicurezza fornendo specifiche tecniche a sostegno dell'attuazione della pertinente normativa dell'Unione, anche in considerazione di un loro possibile richiamo nei sistemi europei di certificazione della cibersicurezza. L'ENISA dovrebbe inoltre monitorare la creazione e l'evoluzione delle norme ad opera dei pertinenti organismi di normazione al fine di seguire le tendenze in materia di normazione a livello europeo e mondiale e, ove necessario, definire tali norme partecipando, anche attraverso l'elaborazione di contributi, alle attività degli organismi di normazione e svolgendovi un ruolo guida. A tal fine, l'ENISA dovrebbe rimanere imparziale. Ad esempio, possono presentarsi situazioni in cui l'ENISA dovrebbe ritirarsi dalle attività pertinenti in seno agli organismi di normazione, qualora le venga chiesto di valutare norme europee che sono state richieste dalla Commissione a sostegno della normativa dell'Unione. L'ENISA non dovrebbe contribuire all'elaborazione delle norme che è incaricata di valutare.
- (42) Per sostenere l'attuazione delle politiche dell'Unione e la preparazione di potenziali attività di normazione, l'ENISA dovrebbe contribuire allo sviluppo e alla valutazione di algoritmi crittografici, in particolare nell'ambito della crittografia post-quantistica. In tale contesto, su richiesta della Commissione e previo accordo di contributo quale definito nel regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio⁵⁰, l'ENISA può istituire un processo per la richiesta e la valutazione di algoritmi specifico per algoritmi crittografici da parte dei pertinenti portatori di interessi, in particolare le comunità crittografiche, accademiche e di ricerca, nonché i fabbricanti, i CSIRT, le autorità nazionali di certificazione della cibersicurezza e le autorità competenti a norma della direttiva (UE) 2022/2555. Qualora contribuisca all'istituzione di tali processi, l'ENISA dovrebbe promuovere la collaborazione tra i pertinenti portatori di interessi e attuare gli aspetti organizzativi. Il processo dovrebbe essere formale, aperto, trasparente e inclusivo, compresa la consultazione dei pertinenti portatori di interessi in merito ai progetti di requisiti minimi e al processo e ai criteri di valutazione, in particolare per quanto riguarda la sicurezza e l'esecuzione delle valutazioni.
- (43) Per sostenere l'attuazione delle attività di valutazione della conformità nell'ambito dei sistemi europei di certificazione della cibersicurezza e di altre normative pertinenti dell'Unione, l'ENISA può fornire pertinenti strumenti tecnici di prova per sostenere gli Stati membri, le imprese e gli organismi di valutazione della conformità nelle attività di valutazione. Tali strumenti dovrebbero mirare a creare sinergie a livello dell'Unione e un funzionamento efficiente delle procedure di valutazione della conformità per rispondere alle esigenze degli Stati membri e del mercato. Tali esigenze possono sorgere, ad esempio, nell'ambito della sicurezza fin dalla progettazione per sostenere le imprese, comprese le piccole e medie imprese, nei loro sforzi di attuazione nel quadro del regolamento (UE) 2024/2847. In tale contesto, l'ENISA dovrebbe riscuotere diritti per coprire i costi pertinenti relativi alla creazione, alla progettazione, allo sviluppo, al mantenimento e all'aggiornamento delle capacità software e hardware necessarie per tali strumenti di prova.

⁵⁰ Regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio, del 23 settembre 2024, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione (GU L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

- (44) Per sostenere gli Stati membri nei loro sforzi volti ad affrontare la carenza di professionisti della cibersecurity e la crescente necessità di una forza lavoro qualificata, diversificata, anche in termini di equilibrio di genere, e agile, e per consentire la mobilità e la preparazione dei lavoratori in tutti gli Stati membri, l'ENISA dovrebbe basarsi sui principi e sul lavoro avviati nell'ambito dell'Accademia per le competenze in materia di cibersecurity. In particolare, l'ENISA dovrebbe istituire il quadro europeo delle competenze in materia di cibersecurity ("ECSF") quale quadro comune per i profili professionali nel settore della cibersecurity. L'ENISA dovrebbe sostenere ulteriormente gli Stati membri nell'affrontare le disparità di genere nei ruoli attinenti alla cibersecurity. Tale approccio è coerente con la visione delineata nella comunicazione della Commissione sull'Unione delle competenze e contribuirebbe al conseguimento dei suoi obiettivi. Dovrebbe essere ulteriormente esaminata la possibilità di un marchio di qualità per gli attestati europei delle competenze individuali in materia di cibersecurity.
- (45) L'ECSF dovrebbe essere uno strumento pratico e flessibile da utilizzare su base volontaria che fornisca una comprensione e una terminologia comuni dei ruoli pertinenti, nonché dei compiti, delle competenze e delle conoscenze associati che sono maggiormente necessari nei ruoli attinenti alla cibersecurity, al fine di contribuire all'individuazione delle competenze critiche, incluse le competenze trasversali, richieste alla forza lavoro e di consentire agli erogatori di istruzione, comprese le imprese, gli istituti di istruzione superiore o gli erogatori di istruzione e formazione professionale, di elaborare programmi e aiutare i responsabili delle politiche a sviluppare iniziative per affrontare le carenze di competenze. Potendo essere utilizzato come quadro di riferimento per il riconoscimento delle competenze, esso dovrebbe anche essere interoperabile con la classificazione europea di abilità/competenze e professioni (*European Classification of Skills and Occupations* – ESCO) al fine di aiutare i dipartimenti delle risorse umane a comprendere i requisiti per la pianificazione delle risorse, le assunzioni e lo sviluppo delle carriere a sostegno delle esigenze in materia di cibersecurity. Laddove il quadro europeo delle competenze digitali per i cittadini (DigComp 3.0) descrive le conoscenze, le competenze e le attitudini necessarie per essere digitalmente competenti per la vita quotidiana, la partecipazione alla società, il lavoro e l'apprendimento e può essere utilizzato sia dagli adulti che dai bambini, l'ECSF offre un quadro semplice che individua i ruoli attinenti alla cibersecurity e i compiti, le conoscenze e le competenze associati necessari per svolgerli. A tale riguardo, si rivolge a un pubblico specializzato in cibersecurity, che spazia dai professionisti della cibersecurity effettivi o potenziali, agli istituti di istruzione e ai datori di lavoro. L'ECSF, essendo lo strumento chiave utilizzato per sviluppare i sistemi, dovrebbe inoltre sostenere lo sviluppo di attestati europei delle competenze individuali in materia di cibersecurity, consentendo l'emergere di nuovi operatori del mercato e contribuendo alla concorrenza sul mercato nell'ambito di un quadro comune. L'ECSF dovrebbe essere valutato e aggiornato periodicamente affinché rifletta adeguatamente le esigenze del mercato del lavoro in materia di cibersecurity e gli sviluppi tecnologici e delle politiche. L'ENISA dovrebbe sostenere la diffusione dell'ECSF da parte degli Stati membri e dei soggetti dell'Unione e al loro interno e fornire un sostegno adeguato laddove sia necessaria assistenza.
- (46) Le competenze e le qualifiche in materia di cibersecurity dovrebbero essere rese comparabili, trasparenti e affidabili in tutto il mercato interno. A tal fine, gli attestati

europei delle competenze individuali in materia di cibersicurezza⁵¹ dovrebbero aiutare i datori di lavoro, comprese le PMI e le start-up, ad assumere effettivi o potenziali professionisti della cibersicurezza in maniera efficace all'interno degli Stati membri e a livello transfrontaliero, in linea con gli obiettivi stabiliti nella comunicazione sull'Unione delle competenze. Al fine di garantire un'attuazione uniforme in tutti gli Stati membri, gli attestati europei delle competenze individuali in materia di cibersicurezza dovrebbero basarsi su una comprensione comune, a livello dell'Unione, delle competenze necessarie per conseguire tali obiettivi e dovrebbero essere rilasciati da soggetti autorizzati dall'ENISA sulla base di una serie comune di criteri. Tale approccio dovrebbe essere coerente con gli obiettivi della futura iniziativa sulla trasferibilità delle competenze e contribuire agli stessi.

- (47) Lo sviluppo di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza dovrebbe mirare a integrare le azioni degli Stati membri offrendo alle autorità pubbliche e agli operatori economici la possibilità di avvalersi di un meccanismo europeo di attestazione, in linea con la competenza di sostegno dell'Unione nel settore dell'istruzione e della formazione professionale di cui all'articolo 6, lettera e), all'articolo 165, paragrafo 1, e all'articolo 166, paragrafo 1, TFUE. I sistemi, insieme all'attività dell'Accademia per le competenze in materia di cibersicurezza, possono anche rappresentare la base per i programmi di istruzione superiore, ad esempio i diplomi europei settoriali, e per lo sviluppo di microcredenziali. Pertanto i sistemi europei di attestazione della cibersicurezza non dovrebbero mirare ad armonizzare le disposizioni legislative e regolamentari degli Stati membri, ma dovrebbero piuttosto essere considerati un fattore abilitante e un'opportunità che gli Stati membri e gli attori economici potrebbero voler cogliere e promuovere.
- (48) L'ENISA dovrebbe garantire che i sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza continuino a rispondere alle esigenze del mercato e si basino sull'esperienza dei soggetti pubblici e privati preposti al rilascio di certificazioni individuali, compresi gli Stati membri, gli istituti di istruzione superiore, gli istituti di istruzione e formazione professionale e le imprese. L'ENISA dovrebbe consultare la Commissione in merito alla definizione delle priorità dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza, tenendo in debita considerazione l'attuazione delle politiche e le esigenze del mercato.
- (49) Per garantire l'allineamento tra l'ECSF e i sistemi, la revisione di un profilo professionale dell'ECSF dovrebbe innescare automaticamente una valutazione dell'idoneità del sistema o dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza associati, e di conseguenza la loro possibile revisione.
- (50) Tenendo conto della diversità dei profili professionali in materia di cibersicurezza e dei compiti, delle competenze e delle conoscenze associati, potrebbe essere necessario adattare la valutazione dei singoli individui e i metodi di valutazione di ciascun sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza. Ciascun sistema dovrebbe garantire che la valutazione delle

⁵¹ Gli attestati europei delle competenze individuali in materia di cibersicurezza dovrebbero essere intesi come basati su un approccio simile a quello che il mercato riconosce come "certificazioni della cibersicurezza". Tuttavia, al fine di evitare confusione per quanto riguarda il quadro europeo di certificazione della cibersicurezza, è preferibile l'espressione "attestazione", già utilizzata nella comunicazione sull'Accademia per le competenze in materia di cibersicurezza.

competenze individuali richieste in termini di risultati dell'apprendimento, compresa, se del caso, la valutazione del livello di competenza, sia sistematicamente effettuata rispetto a un profilo professionale dell'ECSF o di un suo sottoinsieme. I metodi di valutazione possono comprendere elementi quali la verifica delle conoscenze teoriche, esami pratici, prerequisiti e valutazione tra pari. L'esperienza individuale dovrebbe essere tenuta in debita considerazione.

- (51) Al fine di garantire un'attuazione uniforme dei sistemi europei di attestazione delle competenze individuali in materia di cibersecurity, in particolare per quanto riguarda la valutazione dei singoli individui, l'ENISA dovrebbe fornire una formazione obbligatoria al personale incaricato di effettuare tale valutazione. Il personale in questione dovrebbe avere esperienza nel settore della cibersecurity, che potrebbe essere dimostrata dal possesso di un attestato europeo delle competenze individuali in materia di cibersecurity per il profilo professionale per il quale sta effettuando la valutazione e a un livello di competenza almeno equivalente a quello delle persone che sta valutando.
- (52) Il ruolo dei fornitori autorizzati di attestati consiste nell'attestare che una persona è in possesso delle conoscenze e delle competenze per poter svolgere uno dei ruoli definiti dall'ECSF e nel fornire garanzie ai datori di lavoro in tutta l'Unione. Poiché anche i datori di lavoro che gestiscono infrastrutture critiche dell'Unione terrebbero conto della garanzia della qualità delle abilità e delle competenze di coloro che ottengono un attestato europeo delle competenze individuali in materia di cibersecurity, i soggetti autorizzati che attestano il livello di abilità e competenze dovrebbero essere affidabili dal punto di vista della cibersecurity e non dovrebbero essere soggetti all'indebita influenza di un paese terzo che potrebbe destare preoccupazioni per la cibersecurity. Pertanto i soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersecurity designato a norma del presente regolamento o controllati da tale paese terzo, da un soggetto ivi stabilito o da un suo cittadino (fornitori ad alto rischio) a norma del presente regolamento non dovrebbero poter diventare fornitori autorizzati di attestati europei delle competenze individuali in materia di cibersecurity a norma del titolo II, sezione 4.
- (53) Affinché le persone in possesso di un attestato europeo delle competenze in materia di cibersecurity possano utilizzarlo e dimostrarne il possesso con facilità e affinché tale attestato possa essere utilizzato in tutti gli Stati membri, i fornitori autorizzati di attestati dovrebbero garantire che, su richiesta dell'interessato, gli attestati europei delle competenze individuali in materia di cibersecurity siano rilasciati sotto forma di attestati elettronici nel portafoglio europeo di identità digitale (portafoglio EUDI) istituito dal regolamento (UE) n. 910/2014. I fornitori autorizzati di attestati dovrebbero essere considerati prestatori di servizi fiduciari e soggetti al regime di vigilanza e responsabilità di cui al regolamento (UE) n. 910/2014. Il regime per gli attestati di attributi utilizzato a norma del regolamento di esecuzione (UE) 2025/1569 della Commissione⁵² dovrebbe essere registrato nel catalogo dei regimi per gli attestati di attributi di cui a tale regolamento di esecuzione.
- (54) Per contribuire allo sviluppo della forza lavoro nel settore della cibersecurity e alla trasferibilità delle competenze in tutta l'Unione, l'ENISA dovrebbe mettere a disposizione del pubblico i sistemi europei di attestazione delle competenze

⁵² Regolamento di esecuzione (UE) 2025/1569.

individuali in materia di cibersicurezza e l'elenco dei fornitori autorizzati degli attestati attraverso un apposito sito web.

- (55) È opportuno che l'ENISA sia gestita e disciplinata tenendo conto dei principi dell'orientamento comune sulle agenzie decentrate dell'Unione, adottato il 19 luglio 2012 dal Parlamento europeo, dal Consiglio e dalla Commissione⁵³. Le raccomandazioni contenute nell'orientamento comune dovrebbero anche riflettersi, se del caso, nei programmi di lavoro dell'ENISA, nelle sue valutazioni e nelle sue prassi di informazione e amministrazione.
- (56) Affinché possa svolgere efficacemente le sue funzioni, in particolare nel guidare la direzione generale delle attività dell'ENISA e nel definirne le priorità strategiche, è essenziale che il consiglio di amministrazione sia composto da rappresentanti di alto livello degli Stati membri e della Commissione. A tal fine, ciascuno Stato membro dovrebbe nominare quale membro del consiglio di amministrazione la figura di vertice di un'autorità nazionale competente di tale Stato membro responsabile della cibersicurezza designata a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555.
- (57) Per garantire che i supplenti del consiglio di amministrazione possano svolgere adeguatamente il proprio ruolo, gli Stati membri dovrebbero nominare supplenti in possesso di competenze ed esperienza professionali adeguate. Per quanto riguarda i supplenti, la Commissione e gli Stati membri dovrebbero adoperarsi per conseguire una rappresentanza equilibrata di donne e uomini in seno al consiglio di amministrazione e dovrebbero limitarne l'avvicendamento al fine di garantire la continuità dei lavori del consiglio di amministrazione.
- (58) Per consentire all'ENISA di svolgere efficacemente la sua missione, il consiglio di amministrazione, composto da rappresentanti degli Stati membri e della Commissione, dovrebbe stabilire gli orientamenti generali del funzionamento dell'ENISA, comprese le sue priorità strategiche, e garantire che questa svolga i propri compiti conformemente al presente regolamento. Al consiglio di amministrazione dovrebbero essere conferiti i poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'ENISA, adottare il documento unico di programmazione dell'ENISA, adottare il proprio regolamento interno, nominare il direttore esecutivo, decidere in merito alla proroga e alla conclusione del suo mandato, e decidere se creare una funzione di vicedirettore esecutivo e, in tal caso, decidere in merito alla sua nomina, nonché alla proroga e alla conclusione del suo mandato. Chiunque eserciti una funzione esecutiva in seno all'ENISA dovrebbe pertanto essere nominato dal consiglio di amministrazione. Il consiglio di amministrazione dovrebbe inoltre essere responsabile della nomina o della revoca dei membri della commissione di ricorso, nonché della definizione di norme per prevenire o gestire i conflitti di interesse al riguardo.
- (59) Per contribuire a garantire che l'ENISA stabilisca le sue priorità strategiche e le mantenga aggiornate, il consiglio di amministrazione dovrebbe tenere almeno una riunione all'anno dedicata alle priorità strategiche dell'ENISA. Per garantire che le

⁵³ Orientamento comune, allegato alla dichiarazione congiunta del Parlamento europeo, del Consiglio dell'UE e della Commissione europea sulle agenzie decentrate, adottata il 19 luglio 2012 e disponibile all'indirizzo: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

riunioni del consiglio di amministrazione siano efficaci e ben informate, il consiglio di amministrazione può invitare alle sue riunioni qualsiasi persona il cui parere possa essere pertinente e di interesse per gli argomenti discussi, al fine di fornire informazioni, competenze o consulenza. Tale persona sarebbe un osservatore ad hoc senza diritto di voto.

- (60) Salvo disposizione contraria del presente regolamento, il consiglio di amministrazione dovrebbe adottare decisioni a maggioranza assoluta dei suoi membri con diritto di voto. Data l'importanza delle questioni relative al bilancio e alle risorse umane, in particolare per quanto riguarda il bilancio annuale, la relazione annuale di attività, la strategia antifrode, le disposizioni di attuazione per dare effetto allo statuto dei funzionari, la nomina del direttore esecutivo, del vicedirettore esecutivo e del contabile, il seguito dato alle risultanze dell'Ufficio europeo per la lotta antifrode (OLAF) e della Procura europea (EPPO) e l'adozione della regolamentazione finanziaria dell'ENISA, il consiglio di amministrazione dovrebbe adottare tali decisioni solo se il rappresentante della Commissione esprime un voto favorevole. Ai fini dell'adozione di una decisione sull'adozione di un documento unico di programmazione definitivo, tenuto conto del parere della Commissione, il voto favorevole del rappresentante della Commissione dovrebbe essere richiesto soltanto per gli elementi della decisione non correlati al programma di lavoro annuale e pluriennale dell'ENISA.
- (61) Il comitato esecutivo dovrebbe contribuire al funzionamento efficace del consiglio di amministrazione. Nel quadro dei lavori preparatori relativi alle decisioni del consiglio di amministrazione, il comitato esecutivo dovrebbe esaminare dettagliatamente le informazioni pertinenti, valutare le opzioni disponibili e fornire consulenza e soluzioni per la preparazione delle decisioni del consiglio di amministrazione. Dovrebbe inoltre fornire assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione.
- (62) Il corretto funzionamento dell'ENISA esige che il direttore esecutivo sia nominato in base ai meriti e alle comprovate abilità amministrative e manageriali, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza. Le funzioni del direttore esecutivo dovrebbero essere svolte in completa indipendenza. Il consiglio di amministrazione dovrebbe nominare il direttore esecutivo sulla base dell'elenco di candidati preparato dalla Commissione, seguendo una procedura aperta e trasparente che rispetti il principio dell'equilibrio di genere.
- (63) Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di documento unico di programmazione dell'ENISA e adottare tutte le misure necessarie a garantirne l'adeguata attuazione. Il direttore esecutivo dovrebbe redigere una relazione annuale da trasmettere al consiglio di amministrazione che includa l'attuazione del programma di lavoro annuale dell'ENISA, fornire un progetto di stato di previsione delle entrate e delle spese dell'ENISA e dare esecuzione al bilancio. È inoltre opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura scientifica, tecnica, giuridica o socio-economica. Si considera necessaria l'istituzione di un gruppo ad hoc soprattutto per quanto riguarda la preparazione di una specifica proposta di sistema europeo di certificazione della cibersicurezza ("proposta di sistema"). L'istituzione di un gruppo di lavoro ad hoc potrebbe essere necessaria anche per le attività di mantenimento in relazione a specifici sistemi europei di certificazione della cibersicurezza adottati. Dovrebbero inoltre essere istituiti gruppi di lavoro ad hoc per sviluppare e mantenere sistemi europei di attestazione delle competenze

individuali in materia di cibersicurezza e assistere l'Agenzia nella governance, nell'attuazione e nell'evoluzione dell'ECSF. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, con l'intento di garantire un equilibrio di genere e un equilibrio adeguato, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, i soggetti dell'Unione e il settore privato, tra cui le imprese, gli utenti e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione, come pure gli esperti del mondo accademico in materia di prodotti con elementi digitali.

- (64) Il consiglio di amministrazione, se lo ritiene necessario per assicurare o mantenere il buon funzionamento dell'ENISA, può decidere di creare una funzione di vicedirettore esecutivo per assistere il direttore esecutivo. Nel decidere se creare tale funzione, il consiglio di amministrazione può tenere conto del parere del direttore esecutivo.
- (65) È opportuno che l'ENISA disponga di un gruppo consultivo per garantire un dialogo regolare con il settore privato, le organizzazioni dei consumatori e altri soggetti interessati. Il gruppo consultivo ENISA, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'ENISA. Il gruppo consultivo ENISA dovrebbe essere consultato in particolare in merito al progetto di programma di lavoro annuale dell'ENISA. La composizione del gruppo consultivo ENISA e i compiti assegnatigli dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'ENISA. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati e alla vigilanza del mercato nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo di consulenza dell'ENISA.
- (66) I richiedenti che intendono diventare fornitori autorizzati di attestati o rinnovare la propria autorizzazione dovrebbero avere accesso ai mezzi di ricorso necessari qualora siano interessati da decisioni adottate dall'ENISA. Dovrebbe pertanto essere istituito un appropriato meccanismo di ricorso che consenta di impugnare le decisioni dell'Agenzia dinanzi ad una commissione di ricorso, le cui decisioni siano soggette a controllo giudiziario dinanzi alla Corte di giustizia dell'Unione europea conformemente al TFUE. L'obbligo di esperire la procedura di ricorso all'interno dell'ENISA prima di adire la Corte di giustizia dell'Unione europea è applicabile solo alle persone legittimate ad agire dinanzi alla commissione di ricorso.
- (67) Per garantirle piena autonomia e indipendenza e consentirle di svolgere i suoi compiti, è opportuno che l'ENISA sia dotata di un bilancio congruo e autonomo finanziato principalmente da un contributo dell'Unione, ma anche da contributi dei paesi terzi che partecipano alle sue attività e da diritti pagati dai fornitori autorizzati di attestati e dagli organismi di valutazione della conformità che partecipano ai sistemi e rilasciano i certificati europei di cibersicurezza e le dichiarazioni UE di conformità. Allo Stato membro ospitante, e a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente al bilancio dell'ENISA. Nessun contributo, sia esso finanziario o in natura, che l'Agenzia riceva dagli Stati membri, da paesi terzi e da altri soggetti o persone dovrebbe comprometterne l'indipendenza e l'imparzialità. Ai contributi e alle sovvenzioni a carico del bilancio generale dell'Unione dovrebbe applicarsi la procedura di bilancio dell'Unione. Ai fini della trasparenza e della rendicontabilità, la revisione contabile dell'ENISA dovrebbe essere svolta dalla Corte dei conti. Per consentire all'Agenzia di partecipare a tutti i futuri progetti pertinenti, ad essa dovrebbe essere concessa la possibilità di ricevere sovvenzioni.

- (68) Affinché l'ENISA abbia la capacità di rispondere alle richieste per le attività che svolge, in particolare per quanto riguarda le decisioni riguardanti l'autorizzazione al rilascio di attestati europei delle competenze individuali in materia di cibersicurezza e per quanto riguarda il mantenimento dei sistemi europei di certificazione della cibersicurezza e degli strumenti di prova, all'ENISA dovrebbe essere conferito il potere di riscuotere diritti. I diritti associati al trattamento delle domande per diventare un fornitore autorizzato di attestati dovrebbero essere determinati in modo adeguato a contribuire in misura sufficiente a coprire i costi stimati per lo sviluppo e il mantenimento dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza e per valutare se i requisiti e gli obblighi per diventare e continuare a essere un fornitore autorizzato di attestati siano e continuino a essere soddisfatti. I diritti associati ai costi di rilascio e rinnovo delle autorizzazioni dei fornitori autorizzati di attestati dovrebbero includere i costi associati alle valutazioni effettuate dall'ENISA o sotto la sua supervisione. I diritti associati alla partecipazione ai sistemi europei di certificazione della cibersicurezza e per il rilascio di certificati nell'ambito di tali sistemi dovrebbero essere determinati in modo adeguato a contribuire in misura sufficiente a coprire i costi stimati per il mantenimento di tali sistemi. Il pagamento di tali diritti dovrebbe consentire agli organismi di valutazione della conformità notificati e, se del caso, ai titolari di certificati nell'ambito di un sistema di partecipare a tali attività, nonché alle pertinenti attività di sviluppo delle capacità e di promozione, al fine di promuovere lo scambio delle migliori pratiche e favorire l'adozione di sistemi e soluzioni certificate.
- (69) Per garantire la proporzionalità, la trasparenza e la certezza del diritto, i diritti dovrebbero essere fissati in modo trasparente ed equo. Tutte le spese dell'ENISA per il personale impegnato in attività soggette all'imposizione di diritti, in particolare il contributo proporzionale del datore di lavoro al regime pensionistico e i costi relativi alla commissione di ricorso, dovrebbero concorrere alla formazione di tale costo. I diritti non devono determinare l'imposizione di oneri finanziari o amministrativi inutili per richiedenti. È opportuno fissare termini ragionevoli per il pagamento dei diritti.
- (70) È necessario predisporre una serie di indicatori per misurare il carico di lavoro, l'efficacia e l'efficienza dell'Agenzia in relazione alle attività finanziate mediante diritti. Tenendo conto di tali indicatori, l'Agenzia dovrebbe adeguare la pianificazione del personale e la gestione delle risorse relative ai diritti in modo tale da consentire una risposta adeguata a tali richieste e a eventuali variazioni delle entrate derivanti da diritti.
- (71) Per individuare e gestire adeguatamente il rischio di conflitto di interessi reale o percepito, l'ENISA dovrebbe essere tenuta ad adottare regole in materia di prevenzione e gestione dei conflitti di interessi. L'ENISA dovrebbe inoltre applicare le norme in materia di accesso ai documenti di cui al regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio⁵⁴. Il trattamento dei dati personali da parte dell'ENISA dovrebbe avvenire in conformità del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio⁵⁵. È opportuno che l'ENISA si conformi alle

⁵⁴ Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio del 30 maggio 2001 relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43, ELI: <http://data.europa.eu/eli/reg/2001/1049/oj>).

⁵⁵ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n.

disposizioni applicabili ai soggetti dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate UE (ICUE).

- (72) Nello svolgimento dei suoi compiti, l'ENISA può avere accesso a informazioni sensibili, quali le informazioni relative alle minacce e agli incidenti informatici. È pertanto essenziale che l'ENISA tuteli la riservatezza delle informazioni che gestisce. In particolare, in linea con l'articolo 339 del trattato sul funzionamento dell'Unione europea (TFUE), i funzionari e gli altri agenti dell'ENISA, anche dopo la cessazione delle loro funzioni, non dovrebbero divulgare informazioni che per loro natura siano protette dal vincolo del segreto professionale e in particolare quelle relative alle imprese, ai loro rapporti commerciali o agli elementi dei loro costi.
- (73) Per conseguire appieno i propri obiettivi, l'ENISA dovrebbe instaurare rapporti con le autorità di vigilanza dell'Unione e con altre autorità competenti nell'Unione, con i soggetti pertinenti dell'Unione, compresi il CERT-UE, l'EC3 presso Europol, il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, l'Agenzia europea per la difesa (AED), l'Agenzia dell'Unione europea per il programma spaziale (EUSPA), l'organismo dei regolatori europei delle comunicazioni elettroniche (*Body of European Regulators for Electronic Communications* – BEREC), l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE), il comitato europeo per la protezione dei dati, l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (Agency for the Cooperation of Energy Regulators – ACER), l'Agenzia dell'Unione europea per la sicurezza aerea (European Union Aviation Safety Agency – EASA) e con qualsiasi altro soggetto dell'Unione coinvolto nella cibersicurezza. L'ENISA dovrebbe inoltre collaborare con le autorità competenti a norma della direttiva (UE) 2022/2555, le autorità di vigilanza del mercato e le autorità che si occupano di protezione dei dati al fine di scambiare conoscenze e migliori pratiche e dovrebbe fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività.
- (74) Europol svolge un ruolo importante nella prevenzione e nella lotta contro la criminalità informatica, compresa quella connessa agli incidenti di sicurezza delle reti e dell'informazione. Per creare sinergie tra i rispettivi compiti di ciascuna agenzia, l'ENISA dovrebbe cooperare con Europol, in particolare condividendo informazioni sulle tendenze in materia di tecniche, sulle richieste e sugli impatti degli attacchi ransomware. Tale cooperazione può consistere anche nell'individuare i ceppi ransomware più comuni che prendono di mira i soggetti elencati negli allegati I e II della direttiva (UE) 2022/2555 al fine di sostenere i soggetti essenziali e importanti nella risposta e nella ripresa in caso di incidenti.
- (75) Per sostenere la cooperazione operativa e la conoscenza situazionale condivisa delle minacce e degli incidenti informatici, è essenziale che l'ENISA cooperi con i portatori di interessi e in particolare con le imprese e le organizzazioni del settore privato, con le quali può istituire partenariati pubblico-privato.
- (76) Per conseguire efficacemente gli obiettivi delineati nel presente regolamento, l'ENISA può collaborare in particolare con le istituzioni universitarie che hanno avviato

45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

iniziative di ricerca nei settori interessati e sviluppare opportuni canali per i contributi delle organizzazioni dei consumatori e di altre organizzazioni.

- (77) Data la natura transfrontaliera delle minacce e degli incidenti informatici, il livello di cibersicurezza e di preparazione dei paesi terzi può incidere sui soggetti dell'Unione. L'ENISA dovrebbe pertanto essere in grado di fornire attività di sviluppo delle capacità, tra cui attività di formazione, di sviluppo delle capacità e di gemellaggio in paesi terzi, e in particolare attività mirate di sviluppo delle capacità per i paesi candidati all'adesione all'Unione o altri paesi partner, secondo le priorità dell'Unione. Tali attività dovrebbero essere svolte a seguito di una richiesta specifica di fornire un sostegno adeguato, tenendo conto delle priorità dell'Unione, ed essere attuate mediante modalità speciali, anche attraverso accordi di contributo di cui al regolamento (UE, Euratom) 2024/2509. Il quadro europeo di certificazione della cibersicurezza mira a proteggere da minacce informatiche quali un utilizzo fraudolento di vulnerabilità della cibersicurezza o incidenti di cibersicurezza che compromettono la funzionalità (progettazione e funzionamento) dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o la postura di cibersicurezza dei soggetti. Concentrandosi sui rischi tecnici connessi ai prodotti TIC, ai servizi TIC, ai processi TIC, ai servizi di sicurezza gestiti o alla postura di cibersicurezza dei soggetti, il quadro europeo di certificazione della cibersicurezza dovrebbe integrare la sicurezza del quadro per le catene di approvvigionamento delle TIC, che mira a garantire un approccio armonizzato a livello dell'Unione per affrontare i rischi di natura non tecnica nei settori ad alta criticità e in altri settori critici.
- (78) Gli Stati membri dovrebbero poter ricorrere alla certificazione europea della cibersicurezza nel contesto degli appalti pubblici conformemente alla direttiva 2014/24/UE del Parlamento europeo e del Consiglio⁵⁶.
- (79) Per agevolare la semplificazione della conformità per i soggetti, il quadro europeo di certificazione della cibersicurezza dovrebbe prevedere la possibilità di dimostrare la propria postura di cibersicurezza. I soggetti, in particolare quelli che forniscono molteplici tipi di servizi in diversi Stati membri, possono trovarsi di fronte a obblighi diversi in materia di cibersicurezza e sicurezza dei dati a norma di strumenti orizzontali, quali il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio⁵⁷ e la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio⁵⁸, nonché di strumenti settoriali. Al fine di razionalizzare l'attuazione del quadro normativo generale in materia di cibersicurezza e facilitarne il rispetto, la normativa dell'Unione dovrebbe consentire ai soggetti di dimostrare il rispetto degli obblighi in materia di gestione dei rischi di cibersicurezza mediante un certificato europeo di certificazione della cibersicurezza. Un sistema pertinente potrebbe contribuire a razionalizzare i requisiti di conformità derivanti da diversi strumenti normativi, fatte

⁵⁶ Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65, ELI: <http://data.europa.eu/eli/dir/2014/24/oj>).

⁵⁷ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

⁵⁸ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

salve le rispettive prescrizioni specifiche in materia di certificazione. Tali misure di semplificazione possono ridurre gli oneri amministrativi, sbloccando risorse per rafforzare la preparazione operativa in materia di cibersicurezza dei soggetti in settori critici dell'Unione.

- (80) La certificazione europea dei requisiti di gestione dei rischi di cibersicurezza elaborati nell'ambito del quadro europeo di certificazione della cibersicurezza dovrebbe consentire ai soggetti di dimostrare la conformità alla pertinente normativa dell'Unione qualora un sistema contempli i rispettivi obblighi di legge stabiliti in tale atto e qualora preveda tale possibilità. Su tale base, un atto giuridico dell'Unione può anche prevedere una presunzione di conformità a tali requisiti. Tali sistemi potrebbero contribuire a migliorare l'attuazione coerente dei requisiti di cibersicurezza prescritti dalla normativa dell'Unione al fine di garantire condizioni di parità in tutti gli Stati membri e alleggerire l'onere di conformità.
- (81) Il quadro europeo di certificazione della cibersicurezza dovrebbe prevedere la possibilità di certificare i processi TIC, definiti come un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC. Un profilo di protezione è un esempio di processo TIC, come specificato nel regolamento di esecuzione (UE) 2024/482 della Commissione⁵⁹. Un altro esempio di processo TIC è l'insieme di attività intraprese da un fabbricante per progettare e sviluppare in modo sicuro un prodotto TIC, comprese le misure fisiche, logiche, procedurali, relative al personale e altre misure di sicurezza necessarie per proteggere la riservatezza e l'integrità della progettazione e dell'attuazione di un prodotto TIC nel suo ambiente di sviluppo. La certificazione di tali attività è spesso denominata "certificazione del sito" nel contesto di un processo di certificazione a norma del regolamento di esecuzione (UE) 2024/482 della Commissione.
- (82) La definizione di servizi di sicurezza gestiti nel presente regolamento dovrebbe essere coerente con quella di fornitori di servizi di sicurezza gestiti della direttiva (UE) 2022/2555. Tali servizi consistono nello svolgimento di attività legate alla gestione dei rischi in materia di cibersicurezza dei loro clienti o nella fornitura di assistenza per tali attività e hanno acquisito un'importanza crescente nella prevenzione e attenuazione degli incidenti. Di conseguenza i fornitori di tali servizi sono considerati soggetti essenziali o importanti appartenenti a un settore ad alta criticità ai sensi della direttiva (UE) 2022/2555. I fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. Tuttavia i fornitori di servizi di sicurezza gestiti sono stati essi stessi bersaglio di attacchi informatici e presentano un particolare rischio a causa della loro stretta integrazione nelle attività dei clienti. È quindi necessario che i soggetti essenziali e importanti ai sensi della direttiva (UE) 2022/2555 esercitino una maggiore diligenza nella selezione dei fornitori di servizi di sicurezza gestiti.
- (83) I sistemi europei di certificazione della cibersicurezza sono rilevanti per un'ampia comunità di portatori di interessi, quali fornitori di soluzioni TIC, organismi di

⁵⁹ Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCS) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

valutazione della conformità e utenti. Per promuovere un ampio coinvolgimento dei portatori di interessi, è opportuno che almeno una volta all'anno sia organizzata l'assemblea europea sulla certificazione della cibersecurity ("assemblea") con l'obiettivo di promuovere la collaborazione tra la Commissione, l'ENISA, gli Stati membri e i portatori di interessi pertinenti. L'assemblea svolgerà un ruolo centrale nell'individuare e affrontare le nuove sfide e priorità strategiche in materia di cibersecurity per la certificazione e nel garantire che i sistemi di certificazione facilitino l'integrazione sicura delle tecnologie digitali e siano adatti alle esigenze degli utenti. L'assemblea dovrebbe promuovere la leadership dell'Unione nelle attività di certificazione e sostenere la capacità del quadro di certificazione di creare fiducia per le imprese, le autorità pubbliche e il pubblico.

- (84) Al fine di garantire la trasparenza, la Commissione dovrebbe gestire un apposito sito web pubblicando informazioni aggiornate sui progressi compiuti nell'attuazione del quadro europeo di certificazione della cibersecurity. Il sito web dovrebbe contenere informazioni relative ai sistemi di certificazione in fase di preparazione, alle priorità strategiche per i futuri sistemi di certificazione, alle richieste rivolte all'ENISA relative alla preparazione di proposte di sistemi di certificazione e informazioni sull'adozione di sistemi di certificazione. Il sito web della Commissione integrerà il sito web dell'ENISA sui sistemi europei di certificazione della cibersecurity, che dovrebbe offrire dettagli completi sulla preparazione tecnica delle proposte di sistemi e sul loro mantenimento, concentrandosi sui certificati europei di cibersecurity e sulle dichiarazioni UE di conformità rilasciati.
- (85) Al fine di rafforzare il dialogo tra le istituzioni dell'Unione e contribuire a un processo di consultazione formale, aperto, trasparente e inclusivo, la Commissione dovrebbe tenere conto degli elementi derivanti dai pareri espressi dal Parlamento europeo e dal Consiglio e dall'assemblea europea sulla certificazione della cibersecurity in sede di valutazione del presente regolamento.
- (86) Gli studi di fattibilità condotti dall'ENISA dovrebbero essere d'ausilio alla preparazione della pianificazione e dello sviluppo dei sistemi di certificazione della cibersecurity dovrebbero contribuire. Gli studi dovrebbero includere le prospettive dei pertinenti portatori di interessi e allineare i futuri sistemi di certificazione alle attività di ricerca, sviluppo e valutazione tecnologica in corso, riconoscendo in particolare i contributi delle iniziative di ricerca dell'Unione e degli Stati membri. Tali studi possono contribuire a individuare norme e specifiche tecniche disponibili. Essi dovrebbero essere effettuati su richiesta della Commissione o in funzione delle priorità strategiche dell'Unione per garantire che l'evoluzione del panorama tecnologico e le esigenze di cibersecurity siano adeguatamente affrontate e prese in considerazione al momento della richiesta e dello sviluppo dei sistemi.
- (87) La progettazione del sistema proposto e la sua copertura degli obiettivi e degli elementi di sicurezza dovrebbero essere commisurate all'oggetto e all'ambito di applicazione dell'oggetto della certificazione. Ad esempio, un sistema di certificazione dei servizi cloud potrebbe pertanto perseguire obiettivi di sicurezza pertinenti per i servizi TIC e la sicurezza organizzativa. Qualche altro esempio, un obiettivo di sicurezza relativo alla mancata inclusione di vulnerabilità sfruttabili note non sarà probabilmente pertinente per la certificazione dei processi TIC.
- (88) Al fine di garantire che i sistemi europei di certificazione della cibersecurity siano attuati in modo armonizzato in tutti gli Stati membri, è necessario prevedere norme sul mantenimento dei sistemi. Le attività di mantenimento sono inoltre necessarie per

garantire che i sistemi e la relativa documentazione di supporto rimangano aggiornati, in particolare in un settore della cibersicurezza in cui il panorama delle minacce e le tecnologie evolvono costantemente. I sistemi di certificazione dovrebbero pertanto essere concepiti e mantenuti in modo da evitare il rischio di risultare rapidamente obsoleti. Le attività di mantenimento dovrebbero di norma comportare la redazione e l'aggiornamento della documentazione di supporto, comprese le specifiche tecniche e gli orientamenti, nonché l'individuazione di norme o specifiche tecniche pertinenti al sistema. Anche l'analisi del funzionamento del sistema, delle sue potenziali carenze e dei miglioramenti necessari dovrebbe far parte delle attività di mantenimento. Inoltre le attività di mantenimento dovrebbero includere la condivisione di informazioni tra gli Stati membri per quanto riguarda l'attuazione dei sistemi e i contributi ai meccanismi di revisione tra pari e di valutazione tra pari.

- (89) Data la loro natura tecnica, l'ENISA dovrebbe gestire le attività di mantenimento, in cooperazione con la Commissione e con il sostegno del gruppo europeo per la certificazione della cibersicurezza (ECCG) e del relativo sottogruppo per il mantenimento. L'istituzione del sottogruppo dell'ECCG per il mantenimento consente di raccogliere contributi tecnici e informazioni dagli Stati membri al fine di armonizzare gli approcci.
- (90) Le attività di mantenimento dovrebbero comportare interazioni con i pertinenti gruppi di portatori di interessi per garantire che i sistemi rimangano pertinenti per il mercato e aggiornati, anche tramite la condivisione e la ricezione di contributi tecnici. Tali gruppi di portatori di interessi possono essere organizzazioni di normazione, organismi di valutazione della conformità, fornitori, utenti, autorità pubbliche o associazioni di categoria. Le specificità di ciascun sistema, compresi i forum tecnici e le industrie corrispondenti, fanno sì che dovrebbe essere possibile raccogliere contributi tecnici con modalità diverse da un sistema all'altro. Per alcuni sistemi, l'ENISA dovrebbe poter contare su un gruppo di lavoro ad hoc che riunisca esperti delle pubbliche amministrazioni degli Stati membri, dei soggetti dell'Unione e del settore privato. Contributi tecnici potrebbero provenire anche da centri di condivisione e analisi delle informazioni (ISAC) o organizzazioni di normazione. L'ENISA dovrebbe analizzare quale sia il formato più adatto per ciascun sistema e includere una strategia di mantenimento in ciascuna proposta di sistema.
- (91) I sistemi europei di certificazione della cibersicurezza dovrebbero basarsi su norme o specifiche tecniche, in particolare per la definizione dei requisiti di sicurezza e delle metodologie di valutazione. All'ENISA dovrebbe essere data la possibilità di elaborare specifiche tecniche a sostegno della preparazione e del mantenimento dei sistemi, in particolare qualora l'attività delle organizzazioni di normazione non dia risultati o dia risultati non idonei a conseguire gli obiettivi del sistema. Nell'ambito del processo di elaborazione, l'ENISA dovrebbe essere coadiuvata dall'ECCG e, se del caso, dal gruppo di lavoro ad hoc istituito per il sistema pertinente. L'ENISA dovrebbe inoltre chiedere il contributo dei gruppi di portatori di interessi. L'ENISA dovrebbe altresì prendere in considerazione l'accettazione da parte del mercato, nonché le norme europee e internazionali. Tenendo conto della qualità delle specifiche tecniche e degli obiettivi del sistema, la Commissione dovrebbe poter inserire i riferimenti alle specifiche tecniche elaborate dall'ENISA in un sistema europeo di certificazione della cibersicurezza.
- (92) Le specifiche tecniche elaborate dall'ENISA e a cui un sistema fa riferimento dovrebbero essere rese disponibili sul sito web dell'ENISA sui sistemi europei di certificazione della cibersicurezza, in modo che tutte le parti interessate possano

accedervi. Tuttavia, in alcuni casi specifici, la pubblicazione sul sito web potrebbe rappresentare un rischio per la cibersecurity di prodotti TIC, servizi TIC, processi TIC, di servizi di sicurezza gestiti o per la postura di cibersecurity dei soggetti che sono stati certificati e, per estensione, per la sicurezza pubblica. Le specifiche tecniche potrebbero ad esempio contenere informazioni precise su nuovi percorsi di attacco che, se resi disponibili al pubblico, potrebbero essere utilizzati da soggetti malintenzionati. Questo tipo di informazioni dovrebbe essere diffuso in modo limitato in base al principio della necessità di sapere ai portatori di interessi pertinenti, quali le autorità nazionali di certificazione della cibersecurity, gli organismi di valutazione della conformità e i fornitori certificati. Essendo di diffusione limitata, i riferimenti a tali specifiche tecniche non dovrebbero essere inseriti nei sistemi europei di certificazione della cibersecurity e tali specifiche dovrebbero pertanto essere di natura non vincolante.

- (93) I sistemi di certificazione della postura di cibersecurity dovrebbero essere progettati in modo modulare, con l'idea di consentire la dimostrazione della conformità e la presunzione di conformità ai pertinenti requisiti di cibersecurity stabiliti in altre normative dell'Unione, laddove tale normativa preveda tale possibilità. Pertanto la presunzione di conformità ai requisiti previsti in tali atti giuridici avrà effetto come possibile mezzo per dimostrare la conformità solo se i rispettivi atti giuridici consentono tale presunzione di conformità. È pertanto probabile che i dettagli di tale sistema, vale a dire finalità, obiettivi o elementi, differiscano da quelli di altri sistemi. In particolare, dovrebbero essere sviluppati sistemi per la certificazione della postura di cibersecurity dei soggetti al fine di prevedere la valutazione della costante conformità di un soggetto alla normativa dell'Unione. Non è pertanto necessario che i sistemi di certificazione della postura di cibersecurity coprano tutti gli elementi dei sistemi europei di certificazione della cibersecurity, come i livelli di affidabilità, e ciò dovrebbe riflettersi nelle norme relative ai sistemi.
- (94) Un quadro per la certificazione della postura di cibersecurity nell'ambito del quadro europeo di certificazione della cibersecurity consente di sviluppare un sistema che permette ai soggetti che forniscono servizi in diversi Stati membri di dimostrare il rispetto degli obblighi in materia di gestione dei rischi di cibersecurity di cui alla direttiva 2022/2555 del Parlamento europeo e del Consiglio. Su tale base, grazie alla possibilità di dimostrare la conformità, i soggetti possono beneficiare di approcci di vigilanza più coerenti e meno onerosi in tutto il mercato interno. Lo sviluppo di tale sistema di certificazione dovrebbe essere agevolato dall'adozione di atti di esecuzione a norma della direttiva (UE) 2022/2555. Attraverso profili di estensione, un sistema di certificazione della postura di cibersecurity può dimostrare la conformità ai requisiti se uno Stato membro ha adottato o mantenuto in vigore disposizioni che garantiscono un livello più elevato di cibersecurity in linea con la direttiva (UE) 2022/2555. Su tale base, un soggetto che fornisce servizi in diversi Stati membri può dimostrare la conformità a tutti i pertinenti profili di estensione attraverso un unico certificato europeo di cibersecurity.
- (95) Gli obiettivi di sicurezza e i requisiti di sicurezza stabiliti nei sistemi europei di certificazione della cibersecurity per quanto riguarda la sicurezza dei prodotti dovrebbero essere coerenti con i requisiti essenziali di cibersecurity di cui all'allegato I del regolamento (UE) 2024/2847. Tale coerenza è necessaria per garantire che i fabbricanti i cui prodotti rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847 non siano soggetti a requisiti contraddittori quando certificano i loro prodotti nell'ambito di un sistema europeo di certificazione della cibersecurity.

Inoltre la coerenza dei requisiti facilita la presunzione di conformità di cui all'articolo 27 del regolamento (UE) 2024/2847, in base al quale i fabbricanti di prodotti con elementi digitali che sono stati certificati nell'ambito di un sistema europeo di certificazione della cibersecurity possono beneficiare, a determinate condizioni, della presunzione di conformità ai requisiti essenziali di cibersecurity di cui all'allegato I di tale regolamento.

- (96) Nell'ambito del sistema europeo di certificazione della cibersecurity dovrebbe essere possibile specificare un profilo di estensione, stabilendo requisiti aggiuntivi o specifici per i casi d'uso, comprese capacità aggiuntive quali caratteristiche del prodotto migliorate, offerte o risorse di servizi specializzati, processi ottimizzati e misure di sicurezza avanzate. Poiché non corrispondono a uno specifico livello di affidabilità, la finalità dei profili di estensione dovrebbe essere descritta in dettaglio, comprese le minacce alla sicurezza affrontate. I profili di estensione sono intesi in particolare a dimostrare la conformità a norme e requisiti normativi specifici, compresi, se del caso, requisiti riguardanti misure aggiuntive di gestione dei rischi di cibersecurity stabilite da uno Stato membro secondo il principio di armonizzazione minima in linea con la direttiva (UE) 2022/2555.
- (97) Fatto salvo il sistema generale di revisione tra pari che tutte le autorità nazionali di certificazione della cibersecurity devono istituire nell'ambito del quadro europeo di certificazione della cibersecurity, dovrebbe essere possibile includere nei sistemi europei di certificazione della cibersecurity un meccanismo di valutazione tra pari per gli organismi che rilasciano certificati europei di cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersecurity dei soggetti, in particolare per gli organismi che rilasciano certificati con un livello di affidabilità "elevato" nel quadro di tali sistemi. Tali organismi dovrebbero includere anche gli organismi di certificazione delle autorità nazionali di certificazione della cibersecurity che rilasciano certificati con un livello di affidabilità "elevato". L'ECCG dovrebbe sostenere l'attuazione di tali meccanismi di valutazione tra pari. Le valutazioni tra pari dovrebbero in particolare valutare se gli organismi interessati svolgono i rispettivi compiti in maniera armonizzata e possono comprendere meccanismi di impugnazione.
- (98) Crisi quali guerre, catastrofi naturali e pandemie potrebbero ripercuotersi negativamente sulle attività di certificazione. In scenari di crisi di questo tipo, potrebbe non essere possibile, ad esempio, garantire la sicurezza del sito a causa della distruzione delle infrastrutture, di attacchi informatici, di indisponibilità del personale e dell'inaccessibilità del sito. Un sistema europeo di certificazione della cibersecurity dovrebbe pertanto specificare norme temporanee sulla continuità delle attività di certificazione durante scenari di questo tipo.
- (99) La traduzione di proposte di sistemi tecnici in atti di esecuzione richiede conoscenze tecniche e giuridiche complesse e può creare notevoli oneri amministrativi. Inoltre alcuni elementi dei sistemi europei di certificazione della cibersecurity, come la gestione delle vulnerabilità o le condizioni alle quali possono essere utilizzati gli eventuali marchi o etichette, sono intersettoriali e possono trarre vantaggio dall'armonizzazione delle disposizioni di riferimento. Per garantire la qualità dei sistemi europei di certificazione della cibersecurity adottati e ridurre l'onere di conformità per le imprese, alla Commissione dovrebbe essere conferito il potere di adottare disposizioni tipo riguardanti determinati elementi dei sistemi europei di certificazione della cibersecurity.

- (100) Allo scopo di garantire la coerenza del quadro europeo di certificazione della cibersicurezza, in un sistema europeo di certificazione della cibersicurezza dovrebbe essere possibile specificare i livelli di affidabilità per i certificati europei di cibersicurezza e le dichiarazioni UE di conformità rilasciati nell'ambito di detto sistema. Un certificato europeo della cibersicurezza dovrebbe fare riferimento a uno dei livelli di affidabilità: "di base", "sostanziale" o "elevato", mentre la dichiarazione UE di conformità dovrebbe fare riferimento solo al livello di affidabilità "di base". I livelli di affidabilità dovrebbero fornire il rigore e la specificità corrispondenti della valutazione del prodotto TIC, del servizio TIC, del processo TIC, del servizio di sicurezza gestito o della postura di cibersicurezza di un soggetto e dovrebbero essere caratterizzati in riferimento alle specifiche tecniche, norme e procedure correlate, tra cui i controlli tecnici, il cui scopo è attenuare o prevenire gli incidenti. Ciascun livello di affidabilità dovrebbe essere coerente nei vari settori in cui la certificazione si applica.
- (101) La scelta della certificazione appropriata e dei relativi requisiti di sicurezza da parte degli utenti di certificati europei di cibersicurezza dovrebbe basarsi su un'analisi dei rischi associati all'uso di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o sul contesto della certificazione dei soggetti. Pertanto il livello di affidabilità dovrebbe essere commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito, o all'ambiente operativo e alla natura del soggetto la cui postura di cibersicurezza è oggetto di certificazione.
- (102) Per il livello di affidabilità "di base", la valutazione dovrebbe essere guidata almeno dai seguenti componenti di affidabilità: la valutazione dovrebbe comprendere almeno un riesame della documentazione tecnica del prodotto TIC, del servizio TIC, del processo TIC, del servizio di sicurezza gestito o della postura di cibersicurezza di un soggetto da parte dell'organismo di valutazione della conformità. Se la certificazione comprende processi TIC, dovrebbe essere soggetto a riesame tecnico anche il processo utilizzato per la progettazione, lo sviluppo e la manutenzione del prodotto TIC, del servizio TIC, del servizio di sicurezza gestito o della postura di cibersicurezza di un soggetto. Se un sistema europeo di certificazione della cibersicurezza prevede un'autovalutazione della conformità, dovrebbe essere sufficiente che il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, o il soggetto la cui postura di cibersicurezza è oggetto di certificazione, abbia effettuato un'autovalutazione della conformità del prodotto TIC, servizio TIC, processo TIC, servizio di sicurezza gestito o della postura di cibersicurezza di un soggetto al sistema di certificazione.
- (103) Per il livello di affidabilità "sostanziale", la valutazione, oltre ai requisiti per il livello di affidabilità "di base", dovrebbe essere guidata almeno dalla verifica della conformità delle funzionalità di sicurezza del prodotto TIC, del servizio TIC, del processo TIC, del servizio di sicurezza gestito o della postura di cibersicurezza di un soggetto alla documentazione tecnica ad esso relativa.
- (104) Per il livello di affidabilità "elevato", la valutazione, oltre ai requisiti per il livello di affidabilità "sostanziale", dovrebbe essere guidata almeno da un test di efficacia che accerti la resistenza delle funzionalità di sicurezza a ciberattacchi complessi perpetrati da persone che dispongono di abilità e risorse significative. Le attività di valutazione della conformità dovrebbero essere svolte nello Spazio economico europeo per il livello di affidabilità "elevato" o quando un sistema è concepito per dimostrare la conformità e prevedere la presunzione di conformità ad altre normative dell'Unione.

Tale prescrizione è giustificata dal fatto che le attività di valutazione che si svolgono al di fuori dello Spazio economico europeo comportano ulteriori minacce per la cibersecurity, in particolare la proprietà intellettuale dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o dei soggetti valutati. Ad esempio, il codice sorgente di un prodotto TIC potrebbe essere controllato quando attraversa la frontiera di un paese terzo, il che costituisce un rischio per la proprietà intellettuale. Inoltre i laboratori di prova stabiliti in paesi terzi non operano in un ambiente soggetto alle misure di cibersecurity imposte dalla legislazione dell'UE, come la direttiva (UE) 2022/2555 o il regolamento (UE) 2024/2847. Ad esempio, un laboratorio di prova potrebbe avvalersi di un fornitore terzo di servizi cloud che non rispetta i requisiti di cibersecurity di cui alla direttiva (UE) 2022/2555. Tuttavia è opportuno che un sistema di certificazione possa prevedere meccanismi di deroga, ad esempio in relazione alla certificazione dei siti o in altri casi in cui le attività di valutazione della conformità non possono essere ragionevolmente svolte nello Spazio economico europeo.

- (105) In alcuni casi, per conseguire gli obiettivi di sicurezza di un determinato livello di affidabilità, potrebbero essere necessari approcci diversi per rispondere alle specificità di un prodotto TIC, di un servizio TIC, di un processo TIC, di servizi di sicurezza gestiti o di una postura di cibersecurity dei soggetti. Per consentire un approccio più granulare, in un sistema europeo di certificazione della cibersecurity dovrebbe essere possibile specificare uno o più livelli di valutazione corrispondenti a uno dei livelli di affidabilità. Ciò consentirà lo sviluppo di sistemi in cui più livelli di valutazione concepiti per uno scopo diverso corrisponderanno al livello di sicurezza associato a uno specifico livello di affidabilità.
- (106) I sistemi europei di certificazione della cibersecurity dovrebbero poter prevedere che la valutazione della conformità sia effettuata sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, o del soggetto la cui postura di cibersecurity è oggetto di certificazione ("autovalutazione della conformità"). In tal caso dovrebbe essere sufficiente che il fabbricante, il fornitore o il soggetto la cui postura di cibersecurity è oggetto di certificazione effettui tutti i controlli per garantire che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la posizione di un soggetto in materia di deterrenza informatica siano conformi al sistema europeo di certificazione della cibersecurity. L'autovalutazione della conformità dovrebbe essere considerata idonea per prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o per la postura di cibersecurity di un soggetto a bassa complessità, con un basso livello di rischio per l'interesse pubblico e caratterizzati da una progettazione o da meccanismi di produzione semplici.
- (107) Qualora un sistema europeo di certificazione della cibersecurity preveda sia l'autovalutazione della conformità sia la certificazione di prodotti TIC, servizi TIC, processi TIC, di servizi di sicurezza gestiti o della postura di cibersecurity dei soggetti, il sistema di certificazione dovrebbe comprendere mezzi chiari e comprensibili che consentano ai consumatori o altri utenti di distinguere tra i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti, o la postura di cibersecurity dei soggetti che sono stati oggetto di autovalutazione e quelli certificati da terzi.
- (108) I fabbricanti o fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, o i soggetti la cui postura di cibersecurity è oggetto di certificazione, dovrebbero poter rilasciare e firmare la dichiarazione UE di conformità

nell'ambito della procedura di valutazione della conformità. Una dichiarazione UE di conformità è un documento che attesta che uno specifico prodotto TIC, servizio TIC, processo TIC, servizio di sicurezza gestito o la postura di cibersecurity di un soggetto è conforme ai requisiti del sistema europeo di certificazione della cibersecurity. Rilasciando e firmando la dichiarazione UE di conformità, il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, o il soggetto la cui postura di cibersecurity è oggetto di certificazione, si assume la responsabilità della conformità del prodotto TIC, del servizio TIC, del processo TIC, del servizio di sicurezza gestito o della postura di cibersecurity del soggetto ai requisiti di sicurezza del sistema europeo di certificazione della cibersecurity. Una copia della dichiarazione UE di conformità dovrebbe essere trasmessa all'autorità nazionale di certificazione della cibersecurity e all'ENISA.

- (109) I fabbricanti o i fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, o i soggetti la cui postura di cibersecurity è oggetto di certificazione, dovrebbero mettere a disposizione della competente autorità nazionale di certificazione della cibersecurity, per un periodo stabilito nel sistema europeo di certificazione della cibersecurity interessato e conformemente alla normativa dell'Unione applicabile, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità a un sistema europeo di certificazione della cibersecurity. La documentazione tecnica dovrebbe precisare i requisiti applicabili nell'ambito del sistema per quanto rileva ai fini dell'autovalutazione della conformità. La documentazione tecnica dovrebbe essere compilata in modo da permettere di valutare se un prodotto TIC, servizio TIC, processo TIC o un servizio di sicurezza gestito o la postura di cibersecurity del soggetto sia conforme ai requisiti applicabili nell'ambito del sistema.
- (110) I certificati europei di cibersecurity e le dichiarazioni UE di conformità dovrebbero aiutare gli utenti a compiere scelte consapevoli. Le informazioni pertinenti dovrebbero pertanto essere pubblicate su un sito web gestito dall'ENISA. I prodotti TIC, servizi TIC e processi TIC che siano stati certificati o per i quali sia stata rilasciata una dichiarazione UE di conformità dovrebbero pertanto essere accompagnati da informazioni strutturate adeguate al livello tecnico atteso nell'utente previsto. Tutti gli utenti dovrebbero avere accesso alle informazioni relative al numero di riferimento del sistema di certificazione, all'autorità o all'organismo che ha rilasciato il certificato e, se del caso, al livello di affidabilità, o dovrebbero poter ottenere una copia del certificato europeo di cibersecurity. Tali informazioni dovrebbero essere aggiornate periodicamente e rese disponibili su un apposito sito web sui sistemi europei di certificazione della cibersecurity. Inoltre, al fine di garantire la costante accessibilità, i fabbricanti e i fornitori dovrebbero essere tenuti a notificare all'organismo di certificazione competente eventuali cambiamenti nell'ubicazione delle informazioni online o, se del caso, di quelle fisiche.
- (111) La valutazione della conformità è la procedura volta a valutare se siano stati rispettati i requisiti specifici connessi a un prodotto TIC, un servizio TIC, un processo TIC, un servizio di sicurezza gestito o un soggetto. Tale procedura è effettuata da un soggetto terzo indipendente, diverso dal fabbricante o dal fornitore del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito oggetto di certificazione, o dal soggetto la cui postura di cibersecurity è oggetto di valutazione. Un certificato europeo di cibersecurity dovrebbe essere rilasciato qualora la valutazione di un prodotto TIC, servizio TIC, processo TIC, servizio di sicurezza gestito o della postura di cibersecurity del soggetto dia esito positivo. Un certificato europeo di

cibersicurezza dovrebbe essere considerato una conferma della corretta esecuzione della valutazione.

- (112) La rigorosa separazione tra attività di vigilanza e di certificazione è importante per evitare distorsioni e interferenze che potrebbero verificarsi in situazioni in cui il soggetto che vigila sul mercato è anche in concorrenza nello stesso mercato. Di conseguenza, le attività in cui le autorità nazionali di certificazione della cibersicurezza svolgono semplicemente funzioni di vigilanza, ad esempio fornendo la previa approvazione per il rilascio di un certificato, non dovrebbero richiedere un'ulteriore separazione interna dalle altre attività di vigilanza. Ciò comprende, ad esempio, una situazione in cui l'autorità nazionale di certificazione della cibersicurezza raccoglie attivamente informazioni nel corso dell'intero processo di certificazione svolto da organismi privati di valutazione della conformità e successivamente esprime il proprio parere sul rilascio del certificato da parte di tali organismi ("modello di previa approvazione").
- (113) I sistemi europei di certificazione della cibersicurezza dovrebbero specificare le condizioni alle quali potrebbe essere necessario sottoporre nuovamente a certificazione i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersicurezza di un soggetto o alle quali potrebbe essere necessario ridurre l'ambito di applicazione di uno specifico certificato europeo di cibersicurezza. Inoltre i sistemi europei di certificazione della cibersicurezza dovrebbero tenere conto di eventuali effetti negativi dovuti a vulnerabilità o non conformità rilevate successivamente riguardanti i prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti certificati o la postura di cibersicurezza di un soggetto certificato che possono compromettere la conformità ai requisiti di sicurezza di tale certificato.
- (114) L'armonizzazione svolge un ruolo fondamentale nel garantire una cibersicurezza robusta e nel migliorare l'accesso al mercato per le imprese. Al contrario, la frammentazione e la mancanza di riconoscimento reciproco dei certificati creano ostacoli significativi al flusso continuo di dati, aumentando in tal modo i costi operativi per l'industria dell'Unione. Per mitigare tali sfide è essenziale evitare la frammentazione sia nell'ambito dei controlli di sicurezza che nei metodi di valutazione della conformità nel territorio dell'Unione.
- (115) Gli Stati membri dovrebbero informare la Commissione e l'ECCG con sufficiente anticipo prima di adottare nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersicurezza dei soggetti, al fine di aiutare la Commissione e l'ECCG a valutare l'impatto del nuovo sistema nazionale di certificazione della cibersicurezza sul corretto funzionamento del mercato interno, tenendo conto anche dell'eventuale interesse strategico di richiedere un sistema europeo di certificazione della cibersicurezza.
- (116) I riferimenti nella legislazione nazionale a norme nazionali che non sono più applicabili a seguito dell'entrata in vigore di un sistema europeo di certificazione della cibersicurezza possono costituire una fonte di confusione. Gli Stati membri dovrebbero quindi, se del caso, tener conto nella propria legislazione nazionale dell'adozione di un sistema europeo di certificazione della cibersicurezza.
- (117) Al fine di agevolare la crescita di un mercato interno affidabile, creando nel contempo partenariati con i paesi terzi, il processo di certificazione stabilito nel quadro europeo di certificazione della cibersicurezza dovrebbe essere attuato in modo da facilitare il

riconoscimento internazionale, il riconoscimento reciproco e l'allineamento alle norme internazionali.

- (118) Allo scopo di agevolare ulteriormente gli scambi e riconoscendo il carattere internazionale delle catene di approvvigionamento delle TIC, l'Unione può concludere, conformemente all'articolo 218 TFUE, accordi per il reciproco riconoscimento di certificati europei di cibersecurity. Alla Commissione dovrebbe essere conferito il potere di adottare atti di esecuzione per riconoscere unilateralmente l'equivalenza dei certificati di paesi terzi con i certificati europei di cibersecurity. Dovrebbe essere possibile prevedere condizioni specifiche per tale riconoscimento dei certificati di paesi terzi.
- (119) Al fine di conseguire un'attuazione del quadro equivalente in tutta l'Unione, agevolare il riconoscimento reciproco e promuovere l'accettazione generale dei certificati europei di cibersecurity e delle dichiarazioni UE di conformità, è necessario istituire un sistema di revisione tra pari tra le autorità nazionali di certificazione della cibersecurity. La revisione tra pari dovrebbe riguardare le procedure per vigilare sulla conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e della postura di cibersecurity dei soggetti ai certificati europei di cibersecurity, per monitorare gli obblighi dei fabbricanti o fornitori di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti e dei soggetti certificati che effettuano l'autovalutazione della conformità, e per monitorare gli organismi di valutazione della conformità e l'adeguatezza delle competenze del personale degli organismi che rilasciano certificati di livello di affidabilità "elevato". L'ENISA dovrebbe partecipare alle revisioni tra pari in qualità di osservatore e sostenere l'organizzazione del meccanismo di revisione tra pari e delle revisioni stesse, anche elaborando documenti di orientamento e modelli pertinenti, in cooperazione con la Commissione e l'ECCG. L'ENISA dovrebbe inoltre rendere pubblicamente disponibili sul proprio sito web sui sistemi europei di certificazione della cibersecurity le informazioni sul calendario delle revisioni tra pari e l'elenco delle autorità nazionali di certificazione della cibersecurity sottoposte a revisione tra pari che sono tenute a rispettare il calendario. Il regolamento di esecuzione (UE) 2025/2540 della Commissione⁶⁰, adottato a norma del regolamento (UE) 2019/881, stabilisce il piano per le revisioni tra pari utilizzato dai sistemi europei di certificazione della cibersecurity adottati. È necessario garantire il proseguimento delle revisioni tra pari. Tuttavia la Commissione dovrebbe poter stabilire, mediante atti di esecuzione, ove necessario, un nuovo piano per le revisioni tra pari almeno quinquennale, nonché fissare criteri e metodologie per il funzionamento del sistema di revisione tra pari.
- (120) In seguito all'adozione di un sistema europeo di certificazione della cibersecurity, i fabbricanti o fornitori di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o i soggetti la cui postura di cibersecurity è oggetto di certificazione dovrebbero poter presentare domande di certificazione dei loro prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o della loro postura di cibersecurity all'organismo di valutazione della conformità di propria scelta ovunque nell'Unione. Gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo nazionale di accreditamento se soddisfano i requisiti stabiliti nel presente

⁶⁰ Regolamento di esecuzione (UE) 2025/2540 della Commissione, del 9 dicembre 2025, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda la definizione del piano per la valutazione inter pares (GU L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

regolamento e, se del caso, i requisiti specificati dalla Commissione a norma del presente regolamento. Il sistema di cui al presente regolamento dovrebbe essere integrato dal sistema di accreditamento di cui al regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio⁶¹.

- (121) Gli organismi di valutazione della conformità che sono stati accreditati o notificati a norma della legislazione vigente dell'Unione, in particolare il regolamento (UE) 2024/2847 o il regolamento di esecuzione (UE) 2024/482, potrebbero essere in possesso di competenze pertinenti per i sistemi europei di certificazione della cibersecurity di recente adozione. Al fine di evitare inutili oneri finanziari e amministrativi, è opportuno creare sinergie per l'accREDITAMENTO degli organismi di valutazione della conformità a norma del presente regolamento. Per questo motivo i requisiti per l'accREDITAMENTO dei sistemi dovrebbero essere stabiliti in modo tale da garantire il massimo allineamento possibile ai requisiti relativi agli organismi notificati di cui al regolamento (UE) 2024/2847 e ai requisiti per l'accREDITAMENTO di cui al regolamento di esecuzione (UE) 2024/482. Inoltre gli organismi di valutazione della conformità che sono sottoposti a un processo di accREDITAMENTO a norma del presente regolamento dovrebbero poter avvalersi dei risultati di precedenti valutazioni delle loro competenze ai sensi di altre normative dell'Unione, ogniqualvolta vi sia una sovrapposizione dei requisiti per l'accREDITAMENTO.
- (122) Al fine di agevolare la creazione di servizi armonizzati di valutazione della conformità in tutta l'Unione, in un sistema europeo di certificazione della cibersecurity dovrebbe essere possibile stabilire requisiti specifici o supplementari per gli organismi di valutazione della conformità. Nel contesto della certificazione, per autorizzazione si dovrebbe intendere una decisione di un'autorità nazionale di certificazione della cibersecurity che stabilisce che un organismo di valutazione della conformità soddisfa i requisiti specifici o supplementari stabiliti in un sistema europeo di certificazione della cibersecurity per svolgere una specifica attività di valutazione della conformità.
- (123) Qualora un sistema europeo di certificazione della cibersecurity stabilisca requisiti specifici o supplementari a norma del presente regolamento, gli organismi di valutazione della conformità dovrebbero essere autorizzati dalle autorità nazionali di certificazione della cibersecurity a svolgere i compiti previsti da tale sistema. Per evitare autorizzazioni multiple, per aumentare l'accettazione ed il riconoscimento delle decisioni di autorizzazione e per svolgere un controllo efficace degli organismi di valutazione della conformità autorizzati, gli organismi di valutazione della conformità dovrebbero chiedere l'autorizzazione all'autorità nazionale di certificazione della cibersecurity dello Stato membro in cui sono stabiliti. È tuttavia necessario che gli organismi di valutazione della conformità possano chiedere l'autorizzazione in un altro Stato membro qualora nel proprio Stato membro non esista un'autorità nazionale di certificazione della cibersecurity oppure nel caso in cui l'autorità nazionale di certificazione della cibersecurity non abbia le competenze per fornire i servizi di autorizzazione richiesti. È opportuno garantire una cooperazione e uno scambio di informazioni adeguati tra le autorità nazionali di certificazione della cibersecurity. È opportuno che alla Commissione sia conferito il potere di adottare atti di esecuzione

⁶¹ Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accREDITAMENTO e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30, ELI: <http://data.europa.eu/eli/reg/2008/765/oj>).

che stabiliscano le procedure di autorizzazione, anche per quanto riguarda la cooperazione transfrontaliera in materia di autorizzazione.

- (124) Al fine di salvaguardare il livello di protezione richiesto per un prodotto TIC, un servizio TIC, un processo TIC, un servizio di sicurezza gestito o la postura di cibersecurity di un soggetto, è indispensabile che i subappaltatori e le affiliate che si occupano di valutazione della conformità siano tenuti a rispettare gli stessi requisiti applicati agli organismi di valutazione della conformità notificati in relazione allo svolgimento di compiti di valutazione della conformità. Di conseguenza, un organismo di valutazione della conformità dovrebbe disporre delle competenze adeguate ed essere in grado di verificare che i requisiti applicabili siano soddisfatti dai suoi subappaltatori.
- (125) L'autorità di notifica dovrebbe valutare adeguatamente in che misura l'organismo di valutazione della conformità intenda fare affidamento su subappaltatori stabiliti al di fuori dell'Unione o avere accesso a personale o strutture adeguate al di fuori dello Stato membro di notifica. L'autorità pubblica di uno Stato membro dovrebbe avere la possibilità di decidere di non potersi assumere la responsabilità generale di tale accordo in qualità di autorità nazionale di certificazione della cibersecurity e di ritirare o limitare la portata della notifica.
- (126) Al fine di valutare i requisiti di cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti, gli organismi di valutazione della conformità accreditati dovrebbero essere notificati dalle autorità nazionali di certificazione della cibersecurity alla Commissione e agli altri Stati membri. La notifica degli organismi di valutazione della conformità accreditati e, se del caso, autorizzati è indice di affidabilità di tali organismi per lo svolgimento delle attività di valutazione e certificazione conformemente al presente regolamento e al sistema europeo di certificazione della cibersecurity, contribuendo in tal modo alla reputazione generale della certificazione europea della cibersecurity. È pertanto fondamentale garantire che gli organismi di valutazione della conformità che sono stati notificati soddisfino i requisiti e adempiano i loro obblighi nel tempo e che l'elenco degli organismi di valutazione della conformità notificati sia tenuto aggiornato.
- (127) Il regolamento di esecuzione (UE) 2024/3143 della Commissione⁶², adottato a norma del regolamento (UE) 2019/881, stabilisce le circostanze, i formati e le procedure per le notifiche degli organismi di valutazione della conformità utilizzati dai sistemi europei di certificazione della cibersecurity adottati. È pertanto necessario garantire il proseguimento delle attività di notifica. È tuttavia opportuno conferire alla Commissione il potere di adottare atti di esecuzione per adeguare tali circostanze, procedure e formati per la notifica degli organismi di valutazione della conformità. In tale contesto, la Commissione dovrebbe basarsi sull'esperienza acquisita nel contesto dei sistemi esistenti e mirare ad allinearsi ad altre normative e ad altri quadri pertinenti dell'Unione, in particolare al regolamento (UE) 2024/2847 e al nuovo quadro

⁶² Regolamento di esecuzione (UE) 2024/3143 della Commissione, del 18 dicembre 2024, che stabilisce le circostanze, i formati e le procedure per le notifiche a norma dell'articolo 61, paragrafo 5, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersecurity, e alla certificazione della cibersecurity per le tecnologie dell'informazione e della comunicazione (GU L 3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

legislativo, al fine di ridurre l'onere di conformità per gli organismi di valutazione della conformità attivi nell'ambito di diversi strumenti giuridici.

- (128) Le catene di approvvigionamento delle tecnologie dell'informazione e della comunicazione (TIC) sono composte da un insieme collegato di risorse e processi tra operatori economici. Le catene di approvvigionamento delle TIC svolgono una funzione cruciale nel sostenere la stabilità sociale e nel promuovere l'attività economica in tutta l'Unione. Svolgono inoltre un ruolo fondamentale nella realizzazione dell'infrastruttura digitale nell'Unione e sostengono il funzionamento della società e dell'economia dell'Unione. Le catene di approvvigionamento delle TIC consentono la fabbricazione, la produzione, la distribuzione e la manutenzione di servizi TIC, sistemi TIC e prodotti TIC che sono alla base di vari settori critici e altamente critici, tra cui l'assistenza sanitaria, la finanza, i trasporti, le telecomunicazioni, l'energia e le dogane. La sicurezza delle catene di approvvigionamento delle TIC di tali settori critici può anche avere un impatto sulla sicurezza delle infrastrutture militari e di difesa, laddove tali infrastrutture dipendano da settori critici civili e dalle loro catene di approvvigionamento delle TIC. Tuttavia, secondo la relazione sullo stato delle minacce alla cibersecurity pubblicata dall'ENISA (*ENISA Threat Landscape 2025*)⁶³, gli attacchi contro le catene di approvvigionamento sono tra le cinque principali minacce alla cibersecurity, il che dimostra che gli aggressori sfruttano attivamente percorsi indiretti attraverso fornitori terzi e dipendenze. Le perturbazioni delle catene di approvvigionamento delle TIC possono quindi impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto la preparazione e l'efficacia della cibersecurity sono più che mai essenziali per il corretto funzionamento del mercato interno.
- (129) Oltre ai rischi di natura tecnica affrontati dalla direttiva (UE) 2022/55 del Parlamento europeo e del Consiglio⁶⁴, dal regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio⁶⁵ e dal quadro europeo di certificazione della cibersecurity istituito dal regolamento (UE) 2019/881, le catene di approvvigionamento delle TIC sono sempre più esposte a rischi di natura non tecnica. Tali rischi di natura non tecnica possono essere connessi, tra gli altri, a fattori quali la giurisdizione applicabile al fornitore di determinati componenti, in particolare quando un paese terzo o gli autori di minacce controllati da tale paese intraprendono attività di spionaggio economico, conducono attività o campagne informatiche dolose contro l'Unione o i suoi Stati membri o assumono un comportamento irresponsabile nel ciberspazio. I rischi di natura non tecnica possono anche essere collegati a vulnerabilità nascoste o backdoor o a potenziali turbative sistemiche dell'approvvigionamento, in particolare in caso di dipendenza (*lock-in*) tecnologica o dipendenza da determinati fornitori. Ad esempio, i

⁶³ ENISA, *Threat Landscape 2025*, ottobre 2025.

⁶⁴ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>).

⁶⁵ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

meccanismi di emergenza (*kill switch*) potrebbero essere utilizzati per incidere negativamente sulla disponibilità di reti di comunicazione e reti elettriche.

- (130) La comunicazione congiunta "Rafforzare la sicurezza economica dell'UE"⁶⁶ ha sottolineato il rischio che paesi terzi ottengano accesso a informazioni e dati sensibili dell'Unione o dei suoi Stati membri, a seguito di attività di spionaggio industriale, della loro fornitura di hardware o software utilizzati in determinati prodotti o a causa della loro proprietà e del loro controllo di determinate imprese in possesso di informazioni e dati sensibili. Ha inoltre sottolineato il rischio che le infrastrutture critiche dell'Unione, comprese le infrastrutture critiche dei trasporti, dei sistemi spaziali, dell'energia e delle comunicazioni, in particolare quelle individuate come strategiche per la mobilità militare, siano perturbate da soggetti stranieri, il che potrebbe comportare effetti a cascata sull'economia dell'Unione. Le perturbazioni potrebbero verificarsi attraverso attacchi fisici, informatici o ibridi, compreso il sabotaggio di intere strutture o di loro parti o sottocomponenti. Tali perturbazioni potrebbero inoltre essere collegate alle catene di approvvigionamento delle TIC, che forniscono componenti o servizi alla base delle infrastrutture critiche.
- (131) In risposta alle sfide per la sicurezza delle catene di approvvigionamento delle TIC poste dai rischi di natura non tecnica, alcuni Stati membri hanno adottato misure normative, tra cui la designazione di fornitori ad alto rischio, e altri Stati membri faranno probabilmente altrettanto. Ciò potrebbe determinare un aumento delle divergenze negli approcci nazionali e, in ultima analisi, una maggiore vulnerabilità di taluni Stati membri, con potenziali effetti di ricaduta in tutta l'Unione. È pertanto necessario armonizzare alcuni aspetti relativi ai rischi di cibersicurezza di natura non tecnica per la catena di approvvigionamento delle TIC. Tale intervento a livello dell'Unione è giustificato anche dalla necessità di garantire un livello elevato di cibersicurezza in tutta l'Unione. Le disposizioni sulla sicurezza delle catene di approvvigionamento delle TIC mirano a eliminare tali ampie divergenze tra gli Stati membri, in particolare stabilendo norme per i meccanismi di valutazione dei rischi per la sicurezza delle catene di approvvigionamento delle TIC a livello dell'Unione e norme minime di protezione dai rischi per la catena di approvvigionamento delle TIC.
- (132) Al fine di ridurre le dipendenze critiche e le vulnerabilità, è necessario istituire un quadro per catene di approvvigionamento delle TIC affidabili che dovrebbe affrontare i rischi di natura non tecnica connessi a fornitori ad alto rischio e dipendenze in settori ad alta criticità e in altri settori critici. È pertanto necessario fornire un quadro obiettivo, basato sul rischio, adeguato alle esigenze future e tecnologicamente neutro a livello dell'Unione, al fine di individuare le risorse TIC chiave e prevedere una serie di misure di attenuazione proporzionate per affrontare i rischi.
- (133) I rischi per la cibersicurezza, compresi i rischi connessi alla dipendenza da fornitori ad alto rischio, possono essere presenti in diverse catene di approvvigionamento critiche delle TIC nell'Unione, tra cui apparecchiature di rilevamento, veicoli connessi e automatizzati, sistemi di fornitura di energia elettrica e stoccaggio di energia elettrica, sistemi di approvvigionamento idrico, droni e sistemi anti-drone, servizi di cloud computing, dispositivi medici, apparecchiature di sorveglianza, servizi spaziali e semiconduttori. Ad esempio, la presenza di vulnerabilità nelle apparecchiature di rilevamento di sicurezza potrebbe consentire a soggetti malintenzionati di accedere ai

⁶⁶ Comunicazione congiunta al Parlamento europeo e al Consiglio, Rafforzare la sicurezza economica dell'UE (JOIN (2025) 977 final, del 3 dicembre 2025).

sistemi TIC e manipolare gli scanner facendo sì che oggetti vietati possano passare attraverso il punto di controllo di sicurezza senza essere rilevati, con conseguenze potenzialmente catastrofiche.

- (134) Il presente regolamento non dovrebbe impedire agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza per quanto concerne la sicurezza delle catene di approvvigionamento delle TIC, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione. Tali disposizioni possono includere, ad esempio, l'imposizione di misure di attenuazione più rigorose per quanto riguarda le risorse TIC chiave.
- (135) Al fine di individuare i potenziali rischi per la cibersicurezza che interessano specifiche catene di approvvigionamento delle TIC, il gruppo di cooperazione istituito dall'articolo 14 della direttiva (UE) 2022/2555 ("gruppo di cooperazione NIS") può valutare specifiche catene di approvvigionamento delle TIC mediante valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza. Le valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza dovrebbero esaminare, tra l'altro, i principali autori delle minacce, le principali minacce e vulnerabilità che interessano le risorse TIC chiave. Le valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza dovrebbero elaborare un elenco di scenari di rischio e un elenco di misure volte ad attenuare i rischi. Le valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza dovrebbero essere completate entro sei mesi. In caso di urgenza specifica, dovrebbe essere possibile abbreviare i termini.
- (136) Nei casi in cui abbia motivi sufficienti per ritenere che vi sia una minaccia informatica significativa per la sicurezza dell'Unione in relazione alle catene di approvvigionamento critiche delle TIC e che possa essere necessario intervenire per preservare il corretto funzionamento del mercato interno, la Commissione dovrebbe senza indugio consultare gli Stati membri in merito alla necessità di misure di attenuazione ed effettuare una valutazione dei rischi per la sicurezza, tenendo conto della consultazione degli Stati membri.
- (137) Qualora, a seguito di una valutazione dei rischi per la sicurezza condotta dal gruppo di cooperazione NIS o dalla Commissione, risulti che uno specifico paese terzo presenta rischi di cibersicurezza gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione dovrebbe verificare la minaccia rappresentata da tale paese. La Commissione può avviare tale verifica anche sulla base di altre fonti, come una dichiarazione pubblica a nome dell'Unione o di uno Stato membro in risposta a casi di comportamento irresponsabile nel ciberspazio da parte di uno Stato che hanno portato a un incidente di cibersicurezza. Al fine di valutare il livello di minaccia, la Commissione dovrebbe tenere conto di elementi quali l'esistenza di leggi o pratiche nel paese terzo che impongono ai soggetti sottoposti alla sua giurisdizione di comunicare alle autorità di tale paese terzo informazioni sulle vulnerabilità di software o hardware prima che siano noti casi di sfruttamento di tali vulnerabilità. Un altro elemento pertinente è l'assenza di mezzi di ricorso giurisdizionali efficaci e di meccanismi di controllo indipendente e democratico in grado di risolvere le preoccupazioni in materia di sicurezza, anche per quanto riguarda le pratiche esistenti, informazioni circostanziate su incidenti causati da autori di minacce operanti al di fuori del territorio di tale paese che conducono attività o campagne informatiche dolose nonché l'incapacità o la mancata volontà del paese terzo di cooperare con la Commissione o gli Stati membri per affrontare il rischio derivante dalle attività degli autori di tali minacce. La Commissione dovrebbe inoltre

tenere conto delle informazioni derivanti da valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza o da relazioni pubblicate dagli Stati membri o da organizzazioni internazionali quali la NATO.

- (138) Ai fini del presente regolamento, la nozione di controllo dovrebbe essere intesa come la possibilità di esercitare un'influenza determinante su un soggetto giuridico, direttamente o indirettamente attraverso uno o più soggetti giuridici intermedi. Per quanto riguarda i soggetti di un paese terzo che desta preoccupazioni per la cbersicurezza, il controllo dovrebbe essere stabilito anche laddove tale soggetto abbia strutture di gestione esecutiva in tale paese.
- (139) L'Unione non dovrebbe finanziare progetti che coinvolgono fornitori ad alto rischio, che comprometterebbero la sicurezza, gli interessi e la credibilità dell'Unione. I fornitori ad alto rischio individuati a norma del presente regolamento non dovrebbero pertanto avere la facoltà di partecipare ai programmi e agli strumenti di finanziamento dell'Unione attuati in regime di gestione diretta e indiretta conformemente all'articolo 136 del regolamento (UE/Euratom) 2024/2509 e alle norme settoriali dell'Unione, né alle attività di finanziamento dell'Unione attuate in regime di gestione concorrente, anche nell'ambito del prossimo quadro finanziario pluriennale in relazione alla fornitura di componenti TIC o componenti che comprendono componenti TIC da utilizzare in risorse TIC chiave individuate. I partner esecutivi dell'Unione, quali il gruppo Banca europea per gli investimenti e le banche e gli istituti nazionali di promozione, dovrebbero astenersi dal sostenere progetti che contraddicono quanto sopra, anche in operazioni a proprio rischio.
- (140) Gli appalti pubblici possono essere uno strumento efficace che consente alle autorità pubbliche di contribuire a un'economia più innovativa, sostenibile e competitiva e di spendere il denaro pubblico in modo strategico. Gli appalti pubblici relativi a catene di approvvigionamento delle TIC non dovrebbero essere utilizzati a vantaggio di fornitori che minacciano la sicurezza delle infrastrutture critiche dell'Unione. I fornitori ad alto rischio individuati a norma del presente regolamento non dovrebbero pertanto avere la facoltà di partecipare agli appalti pubblici riguardanti la fornitura di componenti TIC o componenti che comprendono componenti TIC da utilizzare in risorse TIC chiave individuate.
- (141) La certificazione della cbersicurezza svolge un ruolo importante nel rafforzare la sicurezza generale e contrastare le minacce informatiche, fungendo da parametro di riferimento per la fiducia. Tale fiducia potrebbe essere minata se gli attestati delle competenze in materia di cbersicurezza fossero rilasciati da fornitori ad alto rischio, che non dovrebbero pertanto avere il diritto di chiedere di diventare soggetti autorizzati al rilascio di attestati delle competenze individuali in materia di cbersicurezza dell'Unione. Analogamente, è altresì opportuno che i fornitori ad alto rischio non possano avere la possibilità di ottenere la certificazione della cbersicurezza nell'ambito del quadro europeo di certificazione della cbersicurezza e di diventare organismi di valutazione della conformità accreditati per il rilascio di tali certificati.
- (142) Le norme in materia di cbersicurezza svolgono un ruolo fondamentale nella sicurezza e nell'affidabilità delle infrastrutture digitali. È necessario adottare misure adeguate per garantire la normazione nel settore della cbersicurezza. Il coinvolgimento di soggetti stabiliti in paesi terzi che sono stati individuati come paesi che destano preoccupazioni per la cbersicurezza in relazione alla catena di approvvigionamento delle TIC in linea con il presente regolamento, o che sono controllati da tali paesi terzi, può far sì che le

norme in materia di cbersicurezza siano influenzate in modo tale da comprometterne la sicurezza e l'affidabilità.

- (143) Sulla base dei risultati delle valutazioni dei rischi per la sicurezza, la Commissione può individuare, mediante atti di esecuzione, quali risorse TIC dovrebbero essere considerate risorse TIC chiave a causa della loro criticità e soggette a specifiche misure di attenuazione. Il mero fatto che la risorsa offra possibilità di connettività dovrebbe essere sufficiente per considerarne i rischi di cbersicurezza.
- (144) Ove necessario per garantire un livello elevato di cbersicurezza, ciberresilienza e fiducia all'interno dell'Unione, le misure di attenuazione possono essere applicate ai soggetti in relazione alla loro catena di approvvigionamento delle TIC e in particolare alle risorse TIC chiave individuate. Le misure di attenuazione proposte dovrebbero basarsi sulla valutazione dei rischi e delle dipendenze potenziali, compreso il potenziale impatto economico e sociale di tali misure sui soggetti interessati che operano in settori altamente critici o in altri settori critici, in particolare le PMI. L'impatto economico dovrebbe considerare i costi di attuazione delle misure di attenuazione, compresa la durata del ciclo di vita dei relativi componenti delle risorse TIC chiave nel caso in cui le misure prevedano anche la sostituzione dei fornitori. Al fine di garantire la continuità della fornitura dei servizi dovrebbe essere anche valutata la disponibilità sul mercato di fornitori alternativi.
- (145) Poiché potrebbero potenzialmente avere un effetto restrittivo sugli scambi internazionali di beni e servizi, le misure di attenuazione dovrebbero essere proporzionate e mirate al fine di perseguire l'obiettivo legittimo di garantire la cbersicurezza delle catene di approvvigionamento delle TIC in relazione ai soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555, in linea con gli obblighi internazionali dell'Unione.
- (146) L'uso, l'installazione o qualsiasi altro tipo di integrazione di componenti forniti da fornitori ad alto rischio nell'ambito di risorse TIC chiave può essere legato a rischi di successivi trasferimenti di dati a un paese terzo. In particolare, una fonte di rischio può essere costituita da un livello insufficiente di protezione dei dati nel paese terzo, ad esempio per quanto riguarda la protezione dei diritti fondamentali, della proprietà intellettuale o dei segreti commerciali, o rispetto all'accesso e allo sfruttamento illeciti di tali dati per eventuali future perturbazioni della catena di approvvigionamento e a fini di spionaggio. Per attenuare tali rischi, possono essere applicate restrizioni in relazione al trasferimento di tipi specifici di dati a paesi terzi.
- (147) La mancanza di diversificazione per quanto attiene alle apparecchiature utilizzate dai soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 genera gravi vulnerabilità. La dipendenza da un unico fornitore crea una dipendenza da apparecchiature o soluzioni specifiche. La mancanza di diversificazione dei fornitori aumenta la vulnerabilità complessiva delle infrastrutture critiche, in particolare se i soggetti acquistano i componenti TIC utilizzati in risorse TIC sensibili da un fornitore che presenta un elevato grado di rischio. La dipendenza incide inoltre in modo significativo sulla resilienza a livello nazionale e dell'Unione e crea singoli punti di vulnerabilità. Per attenuare tali rischi, è possibile applicare l'obbligo di avere più di un fornitore per specifiche risorse TIC chiave.
- (148) È possibile che anche soggetti dell'Unione utilizzino risorse chiave quali definite dal presente regolamento. Pertanto le norme stabilite nel presente regolamento in materia di sicurezza delle catene di approvvigionamento delle TIC dovrebbero essere applicabili anche ad essi. Per garantire che si tenga conto della specificità dei soggetti

dell'Unione, è importante che, quando si effettuano valutazioni coordinate a livello dell'Unione dei rischi, si considerino i rischi di natura non tecnica derivanti dalle catene di approvvigionamento delle TIC per quanto riguarda i soggetti dell'Unione.

- (149) In circostanze eccezionali che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno e qualora vi siano prove chiare che forniscano alla Commissione motivi sufficienti per ritenere che l'utilizzo di componenti TIC o di componenti che comprendono componenti TIC di uno specifico fornitore rappresenti una minaccia significativa per la cibersicurezza delle attività economiche o sociali di almeno tre Stati membri, la Commissione può proporre, in stretta consultazione con gli Stati membri, di vietare l'utilizzo, l'installazione o l'integrazione di tali componenti del fornitore in questione da parte dei soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555.
- (150) Al fine di garantire la proporzionalità delle misure applicate, i soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersicurezza designato a norma del presente regolamento, o controllati da tale paese terzo, da un soggetto ivi stabilito, o da un suo cittadino, possono chiedere di essere esentati dal divieto di fornire a soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 componenti TIC o componenti TIC che comprendono componenti TIC da utilizzare, installare, o integrare in risorse TIC chiave di tale soggetto e di partecipare a procedure di appalto pubblico, organizzate conformemente alla normativa di recepimento delle direttive 2014/24/UE⁶⁷ e 2014/25/UE del Parlamento europeo e del Consiglio⁶⁸ in relazione alla fornitura di componenti TIC o componenti TIC che comprendono componenti TIC da utilizzare in risorse TIC chiave identificate. A tal fine, il soggetto dovrebbe dimostrare con prove chiare di applicare misure efficaci per affrontare i rischi di natura non tecnica e garantire l'assenza di qualsiasi interferenza indebita da parte di un paese terzo che desta preoccupazioni per la cibersicurezza.
- (151) Le reti di comunicazione elettronica costituiscono la struttura portante di una vasta gamma di servizi essenziali per il funzionamento del mercato interno e per il mantenimento e la gestione di funzioni economiche e sociali vitali, quali l'energia, i trasporti, i servizi bancari e sanitari e i sistemi di controllo industriale. Pertanto tali reti altamente critiche rappresentano obiettivi interessanti per tutti i tipi di attacchi informatici e minacce ibride, perturbazioni, attività di spionaggio, raccolta di intelligence, nonché per le frodi e la criminalità finanziaria. La valutazione dei rischi condotta dal gruppo di cooperazione NIS sulla cibersicurezza e la resilienza delle infrastrutture e delle reti di comunicazione europee ha individuato una serie di rischi e minacce di importanza strategica dal punto di vista dell'Unione, quali wiper/ransomware, attacchi, anche alla catena di approvvigionamento, intrusioni nella rete e attacchi distribuiti di negazione del servizio (DDoS).
- (152) In considerazione dell'interconnessione e dell'interdipendenza tra le diverse reti nazionali di comunicazione elettronica, è necessario che tutti gli Stati membri adottino misure adeguate per garantire la sicurezza delle loro reti. Per gli stessi motivi, è

⁶⁷ Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65, ELI: <http://data.europa.eu/eli/dir/2014/24/oj>).

⁶⁸ Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE (GU L 94 del 28.3.2014, pag. 243, ELI: <http://data.europa.eu/eli/dir/2014/25/oj>).

necessario disporre di un quadro giuridico efficace a livello dell'Unione che affronti anche i rischi di natura non tecnica e garantisca la sicurezza delle reti di comunicazione elettronica interconnesse in modo completo.

- (153) In particolare, la cibersicurezza delle reti 5G è una questione di importanza strategica per l'Unione, in quanto tali reti costituiscono la struttura portante di una vasta gamma di servizi di importanza essenziale per il funzionamento del mercato interno e sono inoltre fondamentali per stabilire la nostra prontezza alla difesa, anche in relazione alla mobilità militare. Le reti 5G sono in grado di fornire una connettività ultraveloce affidabile, ad esempio per la condivisione di dati e informazioni, l'individuazione di droni e il coordinamento in tempo reale sul campo di battaglia.
- (154) Il dispiegamento del 5G consiste principalmente in reti non autonome ("*non stand-alone*"), in cui solo la rete di accesso radio è aggiornata alla tecnologia 5G, mentre il resto della rete si affida ancora alle reti centrali 4G esistenti. Le reti 5G non autonome si basano principalmente su infrastrutture già esistenti, il che significa che la sicurezza delle future reti 5G è determinata, in una certa misura, dalle apparecchiature di rete già esistenti e dalla loro configurazione. Pertanto le misure di attenuazione dovrebbero riguardare anche le reti 4G su cui si basa il dispiegamento del 5G.
- (155) Al fine di affrontare importanti sfide in materia di sicurezza nelle reti 5G, gli Stati membri in seno al gruppo di cooperazione NIS, insieme alla Commissione e all'ENISA, hanno effettuato una valutazione coordinata a livello dell'Unione dei rischi per la sicurezza delle reti 5G, esaminando i rischi di natura sia tecnica che non tecnica. Tale valutazione ha individuato diversi rischi, tra cui potenziali interferenze da parte di paesi terzi o soggetti di paesi terzi attraverso la catena di approvvigionamento, e ha classificato le risorse in base alla loro criticità. Tale valutazione dovrebbe essere utilizzata come base per definire le risorse TIC chiave per le reti di comunicazione 5G.
- (156) Per attenuare i rischi individuati nella valutazione coordinata a livello dell'Unione dei rischi per la sicurezza delle reti 5G, il gruppo di cooperazione NIS ha adottato il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G, che stabilisce misure strategiche e tecniche. Sebbene la maggior parte degli Stati membri disponga di quadri giuridici che consentono, come raccomandato nel pacchetto di strumenti per il 5G, di prevedere limitazioni o esclusioni dei fornitori ad alto rischio, l'attuazione di tali quadri non è stata uniforme. Di conseguenza in un numero considerevole di siti 5G nell'Unione sono presenti fornitori ad alto rischio, come indicato nella comunicazione della Commissione sull'attuazione del pacchetto di strumenti per il 5G⁶⁹. Questa situazione crea vulnerabilità, tra cui la dipendenza strategica e la potenziale esposizione a ingerenze da parte di paesi terzi, che potrebbero incidere anche sulle future infrastrutture 6G realizzate partendo dalle reti 5G esistenti. L'attuazione frammentaria delle misure raccomandate nel pacchetto di strumenti per il 5G, in particolare per quanto riguarda l'ambito di applicazione delle limitazioni riguardanti i fornitori ad alto rischio, ha determinato divergenze tra gli Stati membri, il che si traduce in condizioni di disparità che dividono il mercato interno e indeboliscono la sicurezza generale della rete. La Corte dei conti europea ha evidenziato tali disparità, avvertendo che l'assenza di un approccio coordinato compromette il funzionamento del mercato interno. La persistente dipendenza da fornitori ad alto rischio comporta gravi rischi per la sicurezza delle infrastrutture critiche nell'Unione e potrebbe minare

⁶⁹ Comunicazione della Commissione, "Attuazione del pacchetto di strumenti per la cibersicurezza del 5G (C (2023) 4049 final del 15 giugno 2023).

la fiducia nel mercato interno, in quanto livelli di sicurezza disomogenei possono scoraggiare i consumatori e le imprese dall'avvalersi di prodotti e servizi basati sul 5G all'interno dell'Unione. È pertanto essenziale disporre di misure a livello dell'Unione per garantire un approccio armonizzato alla sicurezza delle reti 5G.

- (157) Al fine di stabilire un periodo di eliminazione graduale per le risorse TIC chiave delle reti di comunicazione elettronica fisse e satellitari, la Commissione dovrebbe effettuare una valutazione che tenga debitamente conto del grado dei rischi per la sicurezza connessi a ciascuna specifica risorsa TIC chiave delle reti fisse e satellitari, della durata del ciclo di vita dei componenti pertinenti e dell'impatto economico che l'eliminazione di tali componenti avrebbe sugli operatori interessati. Sulla base dei risultati di tale valutazione, la Commissione può prendere in considerazione la fissazione di diversi periodi di eliminazione graduale per le particolari risorse TIC chiave e i loro elementi integranti.
- (158) Ai fini di un controllo e di un'applicazione efficaci degli obblighi relativi ai fornitori di reti di comunicazione elettronica mobili, fisse e satellitari, le pertinenti autorità competenti ai sensi del presente regolamento dovrebbero garantire una stretta cooperazione con le autorità competenti ai sensi della [proposta di regolamento sulle reti digitali]. Su richiesta di un'autorità competente designata a norma del presente regolamento, le autorità nazionali di regolamentazione o altre autorità competenti per lo spettro radio, se del caso, dovrebbero revocare i diritti di cui all'articolo 9 e all'articolo 20 della [proposta di regolamento sulle reti digitali] se il fornitore di reti pubbliche di comunicazione elettronica non rispetta gli obblighi di cui al presente regolamento, anche nel caso in cui il fornitore non elimini gradualmente i componenti TIC o i componenti che comprendono componenti TIC di fornitori ad alto rischio nell'ambito di risorse TIC chiave entro il periodo specificato conformemente al presente regolamento.
- (159) In considerazione delle differenze esistenti tra le strutture di governance nazionali, gli Stati membri dovrebbero designare o istituire una o più autorità competenti responsabili delle misure di vigilanza ed esecuzione ai sensi del presente regolamento.
- (160) Le autorità competenti dovrebbero fornire sostegno ai soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 ai fini del rispetto degli obblighi loro incombenti a norma del presente regolamento. A tal fine, la Commissione dovrebbe valutare se i fornitori che possono essere interessati da divieti specifici siano stabiliti in un paese terzo che desta preoccupazioni per la cibersicurezza o siano controllati da tale paese terzo o da un soggetto ivi stabilito o da un suo cittadino. Le autorità competenti dovrebbero cooperare strettamente con la Commissione e le altre autorità competenti nell'ambito della rete istituita a norma del presente regolamento. Sulla base della valutazione della Commissione, le autorità competenti dovrebbero condividere le informazioni pertinenti relative ai fornitori ad alto rischio con i soggetti pertinenti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555. I soggetti non sono tenuti a verificare se un fornitore è sotto controllo estero, ma possono fare pieno affidamento sulle informazioni ricevute dalle autorità competenti. Le autorità competenti dovrebbero fare in modo che su tali soggetti non gravino inutili oneri amministrativi.
- (161) Al fine di garantire l'effettiva conformità, il presente regolamento dovrebbe prevedere misure di vigilanza e di esecuzione attraverso le quali le autorità competenti possano vigilare sui soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555. Qualora svolgano i loro compiti di vigilanza ed esecuzione in relazione a tali soggetti,

le autorità competenti dovrebbero limitarsi a quanto necessario e proporzionato per i rischi individuati.

- (162) Al fine di garantire che l'applicazione sia efficace e coerente in tutta l'Unione, è necessario prevedere poteri di esecuzione che le autorità competenti possano esercitare in caso di violazione degli obblighi stabiliti dal presente regolamento. Nell'esercizio di tali poteri di esecuzione, le autorità competenti dovrebbero tenere debitamente conto di diversi elementi, tra cui la natura, la gravità e la durata della violazione, il danno materiale o immateriale causato, il carattere doloso o colposo della violazione, le azioni intraprese per prevenire o attenuare il danno materiale o immateriale, il grado di responsabilità o eventuali violazioni precedenti pertinenti, il grado di cooperazione con l'autorità competente e qualsiasi altro fattore aggravante o attenuante. Le misure di esecuzione, comprese le sanzioni, dovrebbero essere proporzionate e la loro imposizione dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi il diritto a un ricorso effettivo e a un giusto processo, la presunzione di innocenza e i diritti della difesa.
- (163) È altresì importante prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto del tipo di cui agli allegati I o II della direttiva (UE) 2022/2555 di cessare una violazione del presente regolamento conformemente a una precedente decisione dell'autorità competente.
- (164) Al fine di garantire l'efficace applicazione degli obblighi stabiliti nel presente regolamento, ciascuna autorità competente dovrebbe avere il potere di imporre o richiedere l'imposizione di sanzioni.
- (165) Ai fini dell'imposizione di sanzioni a un soggetto del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 che è un'impresa, quest'ultima dovrebbe essere intesa quale impresa conformemente agli articoli 101 e 102 TFUE. Qualora una sanzione pecuniaria sia comminata a una persona che non sia un'impresa, l'autorità competente dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni. L'imposizione di una sanzione non dovrebbe pregiudicare l'applicazione di altri poteri da parte delle autorità competenti.
- (166) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per quanto riguarda l'adozione di atti di esecuzione che stabiliscano norme dettagliate relative ai diritti riscossi dall'ENISA, di atti di esecuzione che prevedano un sistema europeo di certificazione della cibersecurity per prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti, di atti di esecuzione che stabiliscano principi comuni e disposizioni di riferimento volti a definire gli elementi di tutti i sistemi europei di certificazione della cibersecurity, di atti di esecuzione che specifichino le procedure per la previa approvazione o i modelli di delega generale, di atti di esecuzione sul riconoscimento dell'equivalenza dei certificati di cibersecurity di un paese terzo o di un'organizzazione internazionale ai certificati europei di cibersecurity, di atti di esecuzione che definiscano un piano per la revisione tra pari, di atti di esecuzione per stabilire le procedure, anche in materia di cooperazione transfrontaliera, per l'autorizzazione degli organismi di valutazione della conformità, di atti di esecuzione per stabilire le circostanze, i formati e le procedure per le

notifiche degli organismi di valutazione della conformità, di atti di esecuzione che designino un paese terzo come paese che desta preoccupazioni per la cibersecurity delle catene di approvvigionamento delle TIC, di atti di esecuzione che individuino le risorse TIC chiave utilizzate per la fabbricazione di prodotti o la fornitura di servizi da parte di soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555, di atti di esecuzione che impongano nei confronti dei soggetti che operano in settori ad alta criticità e in altri settori critici misure di attenuazione specifiche e specifichino i periodi di tempo per l'eliminazione graduale dei componenti TIC o dei componenti che comprendono componenti TIC forniti da fornitori ad alto rischio, atti di esecuzione che specifichino ulteriormente le condizioni relative all'esenzione per i soggetti stabiliti in un paese terzo o controllati da soggetti di un paese terzo che desta preoccupazioni per la cibersecurity o controllati da soggetti di un tale paese terzo, così come l'adozione di atti di esecuzione che stabiliscano norme dettagliate relative ai diritti riscossi dalla Commissione. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio che sia seguita la procedura d'esame. Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, alla Commissione dovrebbero essere attribuite anche competenze di esecuzione per quanto riguarda la definizione di un elenco di fornitori ad alto rischio interessati da alcune misure previste nel presente regolamento.

- (167) È necessario che i sistemi europei di certificazione della cibersecurity tengano conto dei più recenti sviluppi tecnologici, delle nuove minacce correlate e dell'adozione della nuova normativa dell'Unione che stabilisce che la certificazione europea della cibersecurity possa essere utilizzata per dimostrare la conformità e la presunzione di conformità ai pertinenti requisiti di cibersecurity di tale normativa. Per tali motivi dovrebbe essere delegato alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE al fine di aggiungere o modificare gli obiettivi di sicurezza perseguiti dai sistemi europei di certificazione della cibersecurity. Analogamente, nell'interesse di un quadro per catene di approvvigionamento delle TIC affidabili, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per modificare l'allegato II del presente regolamento al fine di adeguarlo agli sviluppi tecnologici. 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. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.
- (168) L'operato dell'ENISA dovrebbe essere soggetto a una valutazione periodica e indipendente. La valutazione dovrebbe tenere conto del conseguimento degli obiettivi da parte dell'ENISA e della pertinenza dei suoi compiti, in particolare i compiti relativi alla cooperazione operativa a livello di Unione. In caso di riesame, la Commissione dovrebbe valutare in che modo possa essere rafforzato il ruolo dell'ENISA quale punto di riferimento per consulenza e competenze.
- (169) Il regolamento di esecuzione (UE) 2024/482 della Commissione stabilisce norme per quanto riguarda l'adozione del sistema europeo di certificazione della cibersecurity basato sui criteri comuni (EUCC). L'EUCC è il primo e unico sistema europeo di certificazione della cibersecurity adottato a norma del regolamento (UE) 2019/881.

Riguarda la certificazione dei prodotti TIC, compresi i prodotti appartenenti ai settori tecnici "smart card e dispositivi analoghi" e "dispositivi hardware con box di sicurezza", e i profili di protezione (come i processi TIC). È pertanto necessario garantire il proseguimento delle attività di certificazione e delle attività dell'Agenzia.

- (170) Conformemente all'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725⁷⁰, il Garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati e hanno formulato un parere congiunto il [data].
- (171) Il regolamento (UE) 2019/881 dovrebbe essere abrogato.
- (172) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della sua portata e dei suoi effetti, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Titolo I

Disposizioni generali

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento stabilisce:
 - a) la missione, gli obiettivi, i compiti e gli aspetti organizzativi relativi all'Agenzia dell'Unione europea per la cibersicurezza (ENISA);
 - b) un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti, o della postura di cibersicurezza dei soggetti nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione; e
 - c) un quadro affidabile per la catena di approvvigionamento delle TIC.
2. Il quadro di cui al paragrafo 1, lettera b), si applica fatte salve disposizioni specifiche di altri atti giuridici dell'Unione in materia di certificazione volontaria o obbligatoria.
3. Il quadro di cui al primo comma, lettera c), si applica ai soggetti pubblici o privati di un tipo di cui all'allegato I o II della direttiva (UE) 2022/2555 che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione.
4. 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.

⁷⁰ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

Articolo 2 *Definizioni*

Ai fini del presente regolamento si applicano le definizioni seguenti:

- 1) "cibersicurezza": l'insieme delle attività necessarie per proteggere i sistemi informativi e di rete, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;
- 2) "soggetti dell'Unione": soggetti dell'Unione quali definiti all'articolo 3, punto 1), del regolamento (UE, Euratom) 2023/2841;
- 3) "fornitore autorizzato di attestati": un soggetto, pubblico o privato, nei cui confronti l'ENISA ha adottato una decisione che lo autorizza a rilasciare attestati europei delle competenze individuali in materia di cibersicurezza come stabilito in un sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza;
- 4) "attestato europeo delle competenze individuali in materia di cibersicurezza": una registrazione, in formato digitale o fisico, che attesta che una persona conosce, comprende ed è in grado di svolgere i compiti associati a un profilo professionale o a un sottoinsieme di un profilo professionale del quadro europeo delle competenze in materia di cibersicurezza (*European Cybersecurity Skills Framework* – "ECSF"), a seguito di una valutazione prevista da un sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza;
- 5) "sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza": una serie completa di regole, requisiti, norme e procedure stabiliti dall'ENISA e associati a un profilo professionale dell'ECSF o di un suo sottoinsieme, che si applicano ai fornitori autorizzati di attestati e sono da questi applicati;
- 6) "sistema informativo e di rete": un sistema informativo e di rete quale definito all'articolo 6, punto 1), della direttiva (UE) 2022/2555;
- 7) "strategia nazionale per la cibersicurezza": una strategia nazionale per la cibersicurezza quale definita all'articolo 6, punto 4), della direttiva (UE) 2022/2555;
- 8) "incidente": un incidente quale definito all'articolo 6, punto 6), della direttiva (UE) 2022/2555;
- 9) "incidente di cibersicurezza su vasta scala": un incidente di cibersicurezza su vasta scala quale definito all'articolo 6, punto 7), della direttiva (UE) 2022/2555;
- 10) "gestione degli incidenti": la gestione degli incidenti quale definita all'articolo 6, punto 8), della direttiva (UE) 2022/2555;
- 11) "minaccia informatica": qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sui sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone;
- 12) "sistema europeo di certificazione della cibersicurezza": una serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o della postura di cibersicurezza dei soggetti;

- 13) "sistema nazionale di certificazione della cibersecurity": una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity dei soggetti che rientrano nell'ambito di applicazione del sistema specifico;
- 14) "certificato europeo di cibersecurity": un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito, oppure la postura di cibersecurity di un soggetto, è stato oggetto di una valutazione della conformità ai requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersecurity;
- 15) "dichiarazione UE di conformità": un documento rilasciato da un fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o dal soggetto la cui postura di cibersecurity è oggetto di certificazione, in cui si attesta che la conformità ai requisiti corrispondenti al livello di affidabilità "di base", stabiliti nel sistema europeo di certificazione della cibersecurity, è stata dimostrata mediante un'autovalutazione della conformità;
- 16) "prodotto TIC": un elemento o un gruppo di elementi di una di un sistema informativo o di rete;
- 17) "servizio TIC": un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo di sistemi informativi e di rete;
- 18) "processo TIC": un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;
- 19) "servizio di sicurezza gestito": un servizio prestato a un terzo consistente nello svolgimento di attività, o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cibersecurity, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica;
- 20) "accreditamento": l'accreditamento quale definito all'articolo 10, punto 2), del regolamento (CE) n. 765/2008;
- 21) "organismo nazionale di accreditamento": un organismo nazionale di accreditamento quale definito all'articolo 2, punto 11), del regolamento (CE) n. 765/2008;
- 22) "valutazione della conformità": una valutazione della conformità quale definita all'articolo 2, punto 12), del regolamento (CE) n. 765/2008;
- 23) "organismo di valutazione della conformità": un organismo di valutazione della conformità quale definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008;
- 24) "norma": una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio⁷¹;

⁷¹ Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del

- 25) "specifica tecnica": una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012;
- 26) "norma armonizzata": una norma armonizzata quale definita all'articolo 2, punto 1), lettera c), del regolamento (UE) n. 1025/2012;
- 27) "livello di affidabilità": una base per la fiducia nel fatto che un prodotto TIC, servizio TIC, processo TIC, servizio di sicurezza gestito o la posizione di un soggetto in materia di deterrenza informatica soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cbersicurezza, che indica il livello al quale un prodotto TIC, servizio TIC, processo TIC, servizio di sicurezza gestito o la postura di cbersicurezza di un soggetto sono stati valutati, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC, processo TIC, del servizio di sicurezza gestito interessato o della postura di cbersicurezza del soggetto interessato;
- 28) "autovalutazione della conformità": un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti, o dal soggetto la cui posizione in materia di deterrenza è oggetto di certificazione, che valuta se tali prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o la postura di cbersicurezza dei soggetti soddisfino i requisiti di uno specifico sistema europeo di certificazione della cbersicurezza;
- 29) "postura di cbersicurezza dei soggetti": il livello di cbersicurezza dei soggetti rispetto ai requisiti di sicurezza specifici;
- 30) "modello di previa approvazione": un modello in base al quale un organismo di valutazione della conformità può rilasciare un certificato europeo di cbersicurezza sulla base della valutazione di un'autorità nazionale di certificazione della cbersicurezza nel contesto di uno specifico processo di certificazione nell'ambito di un sistema pertinente;
- 31) "modello di delega generale": un modello in base al quale un organismo di valutazione della conformità può rilasciare un certificato europeo di cbersicurezza sulla base di una delega delle attività di certificazione da parte di un'autorità nazionale di certificazione della cbersicurezza;
- 32) "team di risposta agli incidenti di sicurezza informatica" o "CSIRT": un CSIRT designato o istituito a norma dell'articolo 10 della direttiva (UE) 2022/2555;
- 33) "componenti TIC": prodotti TIC, servizi TIC o processi TIC che possono essere utilizzati per il funzionamento delle risorse TIC;
- 34) "risorse TIC": risorse software o hardware presenti nei sistemi informativi e di rete utilizzati da un soggetto de tipo di cui agli allegati I e II della direttiva (UE) 2022/2555;
- 35) "risorse TIC chiave": risorse TIC individuate conformemente all'articolo 102;
- 36) "rete di comunicazione elettronica": una rete di comunicazione elettronica, quale definita all'articolo 2, punto 1), del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali];

Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12, ELI: <http://data.europa.eu/eli/reg/2012/1025/oj>).

- 37) "controllo": la possibilità di esercitare un'influenza determinante su un soggetto giuridico, direttamente o indirettamente, attraverso uno o più soggetti giuridici intermedi;
- 38) "stabilimento": l'esercizio effettivo dell'attività nel quadro di un'organizzazione stabile nel paese in cui il soggetto ha l'amministrazione centrale o il centro di attività principale;
- 39) "fornitore ad alto rischio": uno dei fornitori seguenti:
- a) un soggetto stabilito in un paese terzo che desta preoccupazioni per la cibersicurezza, designato a norma dell'articolo 100 o controllato da tale paese terzo, da un soggetto ivi stabilito o da un suo cittadino;
 - b) un soggetto designato a norma dell'articolo 103, paragrafo 7, e i soggetti da esso controllati;
- 40) "catena di approvvigionamento delle TIC": l'insieme dei servizi TIC, dei prodotti TIC e dei processi TIC che comprende le attività e gli attori coinvolti in tutte le fasi a monte di un prodotto reso disponibile o di un servizio fornito sul mercato;
- 41) "paese terzo": un paese terzo quale definito all'articolo 3, punto 4), del regolamento (UE) 2023/2675 del Parlamento europeo e del Consiglio⁷²;
- 42) "rischio di natura non tecnica": la probabilità che il fornitore sia soggetto all'influenza di un paese terzo in grado di causare la perdita o la perturbazione del servizio fornito o di compromettere il prodotto fabbricato da un soggetto o di determinare l'esfiltrazione di dati, anche a fini di spionaggio o di generazione di entrate;
- 43) "rischio di cibersicurezza di natura non tecnica significativo": un rischio di cibersicurezza di natura non tecnica che si può presumere abbia una probabilità elevata di provocare un incidente che potrebbe avere un impatto negativo grave, causando anche notevoli perdite o perturbazioni materiali o non materiali;
- 44) "funzioni di rete centrale delle reti di comunicazione elettronica mobili": l'elemento centrale dell'architettura delle reti di comunicazione elettronica mobili che collega i principali nodi di rete a internet e gestisce le funzioni essenziali del sistema, tra cui l'autenticazione delle apparecchiature degli utenti, le funzioni di intercettazione legale (LI), i gateway di sicurezza (SeGW) ai margini della rete (*network edge*), le funzioni di segnalazione di sicurezza, il roaming e la gestione delle sessioni, il trasporto di dati nel piano utente e di controllo, la gestione della politica di accesso, la registrazione e l'autorizzazione dei servizi di rete, l'archiviazione dei dati degli utenti finali e della rete, i servizi di rete critici, compreso il sistema dei nomi di dominio (DNS), l'interconnessione con reti mobili di terzi, l'esposizione delle funzioni della rete centrale ad applicazioni esterne, nonché la selezione e la gestione dei segmenti di rete (*slices*);
- 45) "virtualizzazione delle funzioni di rete (NFV) e funzioni di gestione e orchestrazione della rete (MANO) di reti di comunicazione elettronica mobili": il software e l'architettura di base che garantiscono la gestione del ciclo di vita, l'orchestrazione e l'automazione delle funzioni di rete virtualizzate (VNF), delle funzioni di rete

⁷²

Regolamento (UE) 2023/2675 del Parlamento europeo e del Consiglio, del 22 novembre 2023, sulla protezione dell'Unione e dei suoi Stati membri dalla coercizione economica da parte di paesi terzi (GU L, 2023/2675, 7.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2675/oj>).

eseguite nel cloud (CNF) nonché la selezione e la gestione dei segmenti di rete all'interno delle reti di comunicazione elettronica mobile;

- 46) "rete di accesso radio (RAN) delle reti di comunicazione elettronica mobili": la rete che collega le apparecchiature mobili degli utenti alla rete centrale, comprese le stazioni di base (eNodeB per il 4G, gNodeB per il 5G), le unità radio remote (RRH) e le unità di banda base (BBU), i sistemi di antenne attive (AAS) e, se del caso, i componenti RAN disaggregati, quali le unità centralizzate (CU) e le unità distribuite (DU), e il controllore intelligente RAN (RIC);
- 47) "funzioni di rete centrale delle reti di comunicazione elettronica fisse": la logica operativa di base della rete, che collega i principali nodi e gestisce una serie di funzioni essenziali, tra cui l'autenticazione e l'autorizzazione degli utenti (AAA), le funzioni di intercettazione legale (LI), il sistema dei nomi di dominio (DNS) e i servizi di indirizzi IP (DHCP), la gestione della politica di accesso, l'archiviazione dei dati degli utenti finali e della rete, lo smistamento (*switching*) e l'instradamento (*routing*) delle trasmissioni di rete e i gateway internet internazionali (IIG);
- 48) "sistema di gestione della rete delle reti di comunicazione elettronica fisse": tutte le piattaforme centralizzate e i componenti software necessari per il funzionamento, la gestione, la manutenzione e la fornitura della rete e il monitoraggio delle informazioni relative alla rete;
- 49) "funzioni di trasporto e trasmissione delle reti di comunicazione elettronica fisse": tutti i componenti necessari per il backhaul e l'aggregazione del traffico all'interno della rete, comprese le apparecchiature ottiche di trasporto, i collegamenti in ponte radio a microonde e i sistemi di cavi sottomarini che comprendono le apparecchiature subacquee nonché le apparecchiature terminali di linea sottomarine (SLTE) e le strutture fisiche delle stazioni di approdo;
- 50) "rete di accesso delle reti di comunicazione elettronica fisse": la rete che collega i locali dell'utente finale all'aggregazione o alla rete centrale, comprese la terminazione di linea ottica (OLT) e la terminazione di rete ottica (ONT) per le reti in fibra ottica; sistema di terminazione per modem via cavo coassiale (CMTS) e modem via cavo per reti via cavo coassiali e componenti fissi di accesso senza fili se utilizzati come sostituto della linea fissa.

Titolo II

AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA

Capo I

Missione e obiettivi

Articolo 3

Missione dell'ENISA

- 1. La missione dell'ENISA è sostenere gli Stati membri e i soggetti dell'Unione nel conseguimento di un livello elevato di cibersecurity, cyberresilienza e fiducia all'interno dell'Unione.
- 2. L'ENISA funge da punto di riferimento per consulenza e competenze in materia di cibersecurity per gli Stati membri nonché per altri portatori di interessi dell'Unione.

3. Svolgendo i compiti che le sono attribuiti ai sensi del presente regolamento, l'ENISA contribuisce a ridurre la frammentazione nel mercato interno.
4. L'ENISA svolge i compiti che le sono attribuiti dagli atti giuridici dell'Unione
5. L'ENISA sviluppa le proprie capacità, incluse le capacità e abilità tecniche e umane, necessarie al fine di svolgere i compiti attribuiti ai sensi del presente regolamento.

Articolo 4 *Obiettivi dell'ENISA*

1. L'ENISA opera come centro di competenze nel campo della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze, dei contributi e dell'assistenza forniti, alle informazioni che mette a disposizione, alla trasparenza delle procedure, ai metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.
2. L'ENISA assiste gli Stati membri e, se del caso, i soggetti dell'Unione nell'attuazione delle politiche e delle normative orizzontali e settoriali dell'Unione in materia di cibersicurezza, comprese le attività di vigilanza del mercato.
3. L'ENISA fornisce le proprie competenze e assiste la Commissione nell'elaborazione delle politiche e della normativa dell'Unione in materia di cibersicurezza.
4. L'ENISA sostiene lo sviluppo delle capacità e la preparazione nell'Unione, assistendo gli Stati membri, i soggetti dell'Unione, attraverso il servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione (CERT-UE) di cui al capo IV del regolamento (UE, Euratom) 2023/2841, e i portatori di interessi dei settori pubblico e privato nel miglioramento della protezione dei loro sistemi informativi e di rete, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta.
5. L'ENISA contribuisce alla realizzazione dell'Accademia per le competenze in materia di cibersicurezza e alla crescita della forza lavoro nel settore della cibersicurezza nell'Unione sostenendo gli sforzi volti a sviluppare la trasferibilità delle competenze in tutta l'Unione, anche attraverso il mantenimento e la diffusione dell'ECSF e lo sviluppo, il mantenimento e la diffusione di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza conformemente al capo II, sezione 4, del presente titolo, e garantendo l'offerta di formazione a norma dell'articolo 6, paragrafo 8.
6. L'ENISA promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, i soggetti dell'Unione a norma del regolamento (UE, Euratom) 2023/2841, e i portatori di interessi dei settori pubblico e privato su questioni relative alla cibersicurezza.
7. L'ENISA contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella risposta alle stesse.
8. L'ENISA sostiene la cooperazione operativa a livello di Unione, anche contribuendo alla condivisione della conoscenza situazionale del panorama delle minacce e degli incidenti informatici tra gli Stati membri e, in cooperazione con il CERT-UE, tra i soggetti dell'Unione.

9. L'ENISA coopera strettamente con Europol, i CSIRT e altre autorità nazionali competenti al fine di migliorare la preparazione in materia di cibersicurezza e la risposta a incidenti di ransomware.
10. L'ENISA contribuisce all'istituzione e al mantenimento di un quadro europeo di certificazione della cibersicurezza conformemente al titolo III del presente regolamento. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno.
11. L'ENISA contribuisce all'armonizzazione del mercato unico digitale impegnandosi in attività di normazione pertinenti alle politiche dell'Unione in materia di cibersicurezza ed elaborando specifiche tecniche.
12. L'ENISA promuove un elevato livello di consapevolezza in materia di cibersicurezza tra le organizzazioni e le imprese.

Capo II Compiti

Sezione 1 Sostegno all'attuazione delle politiche e della normativa dell'Unione

Articolo 5

Sostegno all'attuazione delle politiche e della normativa dell'Unione

1. L'ENISA contribuisce all'attuazione delle politiche e della normativa dell'Unione:
 - a) assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, anche emanando orientamenti tecnici e relazioni, fornendo consulenza e condividendo migliori pratiche, nonché agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;
 - b) agevolando la condivisione di informazioni intra e intersettoriale, in particolare per quanto riguarda i settori che figurano negli allegati I e II della direttiva (UE) 2022/2555 e i prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847, fornendo migliori pratiche e orientamenti sugli strumenti e sulle procedure disponibili;
 - c) su richiesta della Commissione, assistendo gli Stati membri mediante la fornitura di sostegno, ad esempio orientamenti tecnici, anche in merito alle misure di gestione dei rischi di cibersicurezza, strumenti per la valutazione di maturità della cibersicurezza e manuali di risposta agli incidenti, adattati ai settori che figurano negli allegati I e II della direttiva (UE) 2022/2555, o di sostegno per l'attuazione di principi di sicurezza fin dalla progettazione per i prodotti con elementi digitali conformemente al regolamento (UE) 2024/2847, al fine di agevolare il miglioramento dei livelli di maturità della cibersicurezza e la conformità al diritto dell'Unione in materia di cibersicurezza;
 - d) contribuendo ai lavori del gruppo di cooperazione istituito a norma dell'articolo 14, paragrafo 1, della direttiva (UE) 2022/2555 ("gruppo di cooperazione NIS"), del gruppo di cooperazione per l'identità digitale europea istituito a norma dell'articolo 46 sexies, paragrafo 1, del regolamento (UE) n. 910/2014,

del gruppo europeo per la certificazione della cibersecurity ("ECCG") di cui all'articolo 90 del presente regolamento e del gruppo di cooperazione amministrativa (ADCO) istituito a norma dell'articolo 52, paragrafo 15, del regolamento (UE) 2024/2847;

- e) assistendo gli Stati membri e i soggetti pertinenti dell'Unione nello sviluppo e nella promozione di politiche sulla cibersecurity che sostengano la disponibilità generale e l'integrità del carattere pubblico di una rete internet aperta, che ne costituisce un aspetto essenziale;
 - f) conformemente al regolamento (UE) 2024/2847, fornendo consulenza e sostegno tecnici agli Stati membri e alla Commissione su questioni relative all'attuazione di tale regolamento;
 - g) assistendo gli Stati membri nello svolgimento dell'assistenza reciproca e nell'agevolazione di tali processi di cooperazione per i soggetti essenziali e importanti a norma dell'[articolo 37 bis della direttiva (UE) 2022/2555];
 - h) su richiesta del comitato europeo per la protezione dei dati, fornendo consulenza sull'attuazione di aspetti specifici relativi alla cibersecurity delle politiche e del diritto dell'Unione in materia di protezione dei dati e della vita privata.
- 2. L'ENISA contribuisce alle valutazioni coordinate a livello dell'Unione dei rischi per la cibersecurity, comprese quelle effettuate a norma dell'articolo 22 della direttiva (UE) 2022/2555.
 - 3. L'ENISA emana orientamenti relativi all'interoperabilità dei sistemi informativi e di rete per la condivisione delle informazioni, anche per quanto riguarda i poli informatici transfrontalieri di cui all'articolo 6, paragrafo 3, del regolamento (UE) 2025/38.
 - 4. L'ENISA è membro del gruppo di cooperazione NIS a norma dell'articolo 14, paragrafo 3, della direttiva (UE) 2022/2555.
 - 5. Su richiesta della Commissione, l'ENISA fornisce competenze, consulenza tecnica, informazioni o analisi o svolge lavori preparatori su specifiche questioni di cibersecurity al fine di orientare l'elaborazione delle politiche della Commissione e il monitoraggio dell'attuazione della legislazione dell'Unione.

Articolo 6

Sviluppo delle capacità

L'ENISA assiste:

- 1) gli Stati membri nell'impegno a migliorare la prevenzione, la rilevazione e l'analisi delle minacce informatiche e degli incidenti, come pure la capacità di risposta agli stessi, fornendo loro le conoscenze e le competenze necessarie;
- 2) gli Stati membri, su loro richiesta, nella definizione e attuazione di politiche di divulgazione delle vulnerabilità su base volontaria;
- 3) conformemente al regolamento (UE, Euratom) 2023/2841, il CERT-UE e il comitato interistituzionale per la cibersecurity, nell'impegno a sostenere i soggetti dell'Unione nel rafforzamento della loro cibersecurity, a migliorare la prevenzione, il rilevamento e l'analisi delle minacce e degli incidenti

informatici nonché a migliorare le loro capacità di risposta a tali minacce e incidenti informatici;

- 4) gli Stati membri nello sviluppo di CSIRT nazionali, ove richiesto a norma dell'articolo 10, paragrafo 10, della direttiva (UE) 2022/2555;
- 5) gli Stati membri nello sviluppo, o nell'aggiornamento, di una strategia nazionale per la cibersecurity e di indicatori chiave di prestazione per la valutazione di tale strategia, ove richiesto a norma dell'articolo 7, paragrafo 4, della direttiva (UE) 2022/2555, e promuove la diffusione di tali strategie in tutta l'Unione e prende nota dei progressi compiuti nella loro attuazione allo scopo di promuovere le migliori pratiche;
- 6) le istituzioni dell'Unione, su loro richiesta, nello sviluppo e nella revisione di strategie dell'Unione in materia di cibersecurity, nella promozione della loro diffusione e nel monitoraggio dei progressi compiuti nella loro attuazione;
- 7) i CSIRT nazionali nell'innalzare il livello delle loro capacità, anche attraverso la promozione del dialogo e degli scambi di informazioni, al fine di assicurare che, tenuto conto dello stato dell'arte, tutti i CSIRT possiedano una serie comune di capacità minime e operino secondo le migliori pratiche;
- 8) gli Stati membri, i soggetti dell'Unione e i portatori di interessi dei settori pubblico e privato nei loro sforzi volti a valutare, accrescere e migliorare la forza lavoro nel settore della cibersecurity, anche sviluppando e mantenendo gli strumenti pertinenti, quali l'ECSF e i sistemi europei di attestazione delle competenze individuali in materia di cibersecurity conformemente alla sezione 4 del presente capo, e promuovendone l'adozione;
- 9) gli organismi pubblici competenti e i portatori di interessi del settore privato, organizzando attività di formazione mirate, se del caso in cooperazione con i portatori di interessi;
- 10) il gruppo di cooperazione NIS nello scambio di migliori pratiche e informazioni, in particolare in relazione all'attuazione della direttiva (UE) 2022/2555 a norma dell'articolo 14, paragrafo 4, lettera c), di tale direttiva;
- 11) le autorità di vigilanza del mercato designate a norma del regolamento (UE) 2024/2847 nelle loro attività volte a garantire l'efficace attuazione di tale regolamento, compreso il sostegno per gli orientamenti e la consulenza tecnica per gli operatori economici, il sostegno per la verifica della conformità, la valutazione dei rischi, le attività congiunte e le indagini a tappeto di cui al regolamento (UE) 2024/2847;
- 12) i membri dell'ECCG nello scambio delle migliori pratiche e, su richiesta dei singoli Stati membri, assiste le autorità nazionali di certificazione della cibersecurity in relazione all'attuazione dei sistemi europei di certificazione della cibersecurity a livello nazionale;
- 13) le autorità pubbliche e i portatori di interessi del settore privato in relazione alle attività di valutazione della conformità, compresi gli organismi di valutazione della conformità e le piccole e medie imprese, al fine di contribuire a un ecosistema di valutazione della conformità solido, competitivo, inclusivo e armonizzato a sostegno dell'attuazione del regolamento (UE) 2024/2847 e del quadro europeo di certificazione della cibersecurity;

- 14) il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento istituiti a norma del regolamento (UE) 2021/887, condividendo informazioni sui rischi e sulle minacce informatiche attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti;
- 15) gli Stati membri, fornendo sostegno tecnico, anche per l'istituzione e il funzionamento di spazi di sperimentazione normativa nel settore della cibersicurezza conformemente alla pertinente legislazione dell'Unione.

Articolo 7

Sensibilizzazione e bacino di talenti

L'ENISA assiste gli Stati membri nei loro sforzi di sensibilizzazione in merito alle politiche e alla normativa dell'Unione in materia di cibersicurezza e ne promuove la visibilità sviluppando strumenti e orientamenti attuabili. L'ENISA sostiene iniziative volte ad ampliare il bacino europeo di talenti nel settore della cibersicurezza, in particolare attraverso il coordinamento dei concorsi.

Articolo 8

Conoscenza e analisi del mercato

1. L'ENISA effettua e diffonde analisi delle principali tendenze del mercato della cibersicurezza sia dal lato della domanda che da quello dell'offerta, in particolare per quanto riguarda i settori in cui esistono o sono previsti sistemi europei di certificazione della cibersicurezza, i settori che figurano negli allegati I e II della direttiva (UE) 2022/2555 e le categorie di prodotti disciplinate dal regolamento (UE) 2024/2847, compresi gli allegati III e IV di tale regolamento.
2. L'ENISA effettua e diffonde analisi delle tendenze tecnologiche in materia di cibersicurezza, in particolare in relazione alle attività e ai soggetti che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 e ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847.
3. L'ENISA sviluppa conoscenze e diffonde consulenze tecniche e analisi su strumenti, norme quadro e migliori pratiche all'avanguardia in materia di cibersicurezza.

Articolo 9

Cooperazione internazionale

L'ENISA contribuisce all'impegno dell'Unione nella cooperazione con i paesi terzi e le organizzazioni internazionali, nonché all'interno dei pertinenti quadri di cooperazione internazionale, per promuovere la cooperazione internazionale sulle questioni connesse alla cibersicurezza:

- a) impegnandosi, ove opportuno, in qualità di osservatore e nell'organizzazione delle esercitazioni internazionali, nonché analizzando i risultati di tali esercitazioni e comunicandoli al consiglio di amministrazione;
- b) agevolando, su richiesta della Commissione, lo scambio di migliori pratiche con paesi terzi e organizzazioni internazionali;

- c) fornendo competenze specialistiche alla Commissione, su richiesta della stessa;
- d) fornendo consulenza specialistica e assistenza alla Commissione su questioni relative al riconoscimento internazionale dei certificati europei di cibersecurity conformemente all'articolo 87;
- e) fornendo consulenza specialistica e assistenza alla Commissione su questioni concernenti la normazione internazionale e collaborando con le pertinenti organizzazioni internazionali di normazione, se del caso, in collaborazione con l'ECCG istituito a norma dell'articolo 90.

Sezione 2

Cooperazione operativa

Articolo 10

Cooperazione operativa a livello di Unione

1. L'ENISA sostiene la cooperazione operativa tra gli Stati membri, i soggetti dell'Unione attraverso il CERT-UE, e tra gli altri portatori di interessi.
2. L'ENISA è membro della rete di CSIRT nazionali istituita a norma dell'articolo 15, paragrafo 1, della direttiva (UE) 2022/2555 e ne assicura il segretariato a norma dell'articolo 15, paragrafo 2, della direttiva (UE) 2022/2555.
3. L'ENISA assicura il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) a norma dell'articolo 16, paragrafo 2, secondo comma, della direttiva (UE) 2022/2555.
4. L'ENISA sostiene la cooperazione tecnica e operativa tra gli Stati membri, in particolare attraverso la rete di CSIRT ed EU-CyCLONe. Tale sostegno comprende:
 - a) la fornitura di consulenza per il miglioramento delle capacità di prevenire e rilevare gli incidenti, nonché di rispondervi e di riprendersi dagli stessi;
 - b) su richiesta di uno o più Stati membri, la fornitura di consulenza e valutazioni in relazione a uno specifico incidente informatico o una specifica minaccia informatica, potenziale o in corso, anche tramite la messa a disposizione di competenze e l'agevolazione della gestione tecnica di tali incidenti, e il sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri;
 - c) l'esecuzione di analisi delle vulnerabilità, delle minacce e degli incidenti;
 - d) su richiesta di uno o più Stati membri, la fornitura di sostegno in relazione a indagini tecniche ex post sugli incidenti significativi ai sensi dell'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555;
 - e) un contributo al sostegno della gestione coordinata degli incidenti e delle crisi di cibersecurity su vasta scala a livello operativo, in particolare assistendo EU-CyCLONe nella preparazione di relazioni destinate ai responsabili politici e agevolando la condivisione tempestiva delle informazioni tra la rete di CSIRT e EU-CyCLONe.
5. Su richiesta di uno Stato membro o di un soggetto dell'Unione in cooperazione con il CERT-UE, l'ENISA sostiene una comunicazione pubblica coerente in merito a un incidente o a una minaccia informatica.

6. L'ENISA sostiene la cooperazione tra gli Stati membri e, attraverso il CERT-UE, tra i soggetti dell'Unione per quanto riguarda la diffusione di strumenti di comunicazione sicura. Nell'ambito della rete di CSIRT e di EU-CyCLONe, l'ENISA usa strumenti di comunicazione sicura forniti da soggetti giuridici stabiliti o considerati stabiliti nell'Unione e controllati da Stati membri o da cittadini di Stati membri.

Articolo 11

Conoscenza situazionale condivisa in materia di cibersicurezza

1. Ai fini di una migliore conoscenza situazionale condivisa del panorama delle minacce e degli incidenti informatici tra gli Stati membri e tra i soggetti dell'Unione, l'ENISA:
 - a) sviluppa, in cooperazione con EU-CyCLONe, la rete di CSIRT, la Commissione, il CERT-UE, Europol e altri soggetti pertinenti dell'Unione, archivi verificati e affidabili dell'intelligence sulle minacce informatiche, che contemplano anche le tendenze in materia di incidenti, tattiche, tecniche e procedure;
 - b) a norma dell'articolo 12, emette allerte precoci in caso di incidente significativo o su vasta scala, potenziale o in corso, o di minaccia informatica di potenziale natura transfrontaliera, in particolare in relazione ai settori elencati negli allegati I e II della direttiva (UE) 2022/2555;
 - c) fornisce, su richiesta della rete di CSIRT, di EU-CyCLONe o della Commissione, analisi tempestive ad hoc sulle tendenze emergenti in materia di incidenti;
 - d) fornisce, su richiesta degli Stati membri o della Commissione, analisi o altre informazioni riguardanti un rischio o una minaccia per la cibersicurezza effettivi o percepiti;
 - e) fornisce analisi e consulenza tecnica in merito ai rischi di cibersicurezza nei prodotti con elementi digitali, anche a sostegno della vigilanza del mercato e redigendo una relazione tecnica biennale sulle tendenze emergenti conformemente all'articolo 17, paragrafo 3, del regolamento (UE) 2024/2847;
 - f) elabora periodicamente una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatiche e mette tale relazione a disposizione del Consiglio, di EU-CyCLONe, della rete di CSIRT, della Commissione, del servizio europeo per l'azione esterna e di Europol;
 - g) monitora le tendenze relative alle tecniche, alle richieste e all'impatto degli attacchi ransomware e fornisce informazioni su tali tendenze alla Commissione, alla rete di CSIRT, a EU-CyCLONe e a Europol.
2. Ai fini di una migliore conoscenza situazionale condivisa del panorama delle minacce e degli incidenti informatici tra i portatori di interessi, l'ENISA:
 - a) effettua analisi delle minacce informatiche, degli incidenti, delle tendenze, delle tecnologie emergenti e del loro impatto, compresa un'analisi periodica riguardante i settori elencati negli allegati I e II della direttiva (UE) 2022/2555 e le pertinenti categorie di prodotti disciplinate dal regolamento (UE) 2024/2847;

- b) fornisce, in cooperazione con la Commissione e, se del caso, con la rete di CSIRT, consulenza, orientamenti e migliori pratiche per la sicurezza dei sistemi informativi e di rete, in particolare per la sicurezza delle infrastrutture su cui poggiano i settori di cui agli allegati I e II della direttiva (UE) 2022/2555;
 - c) effettua analisi strategiche a lungo termine delle minacce informatiche e degli incidenti al fine di individuare le tendenze emergenti e contribuire a prevenire gli incidenti;
3. L'ENISA può rendere pubbliche le analisi, le consulenze, gli orientamenti, le migliori pratiche e le relazioni di cui al paragrafo 2, in accordo con i soggetti che vi hanno contribuito di cui al paragrafo 2.
4. Nello svolgimento delle attività elencate al paragrafo 1, lettere da a) a d) ed f), e al paragrafo 2, l'ENISA utilizza le proprie analisi e, se del caso, le informazioni ricevute nello svolgimento dei propri compiti, tra cui:
- a) informazioni rese disponibili in fonti accessibili al pubblico, comprese le vulnerabilità pubblicamente note nei prodotti TIC o nei servizi TIC disponibili nella banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555;
 - b) informazioni condivise da Stati membri, soggetti dell'Unione, CERT-UE, partner del settore privato o non governativi e paesi terzi e organizzazioni internazionali, fatte salve eventuali limitazioni, segnalate con un contrassegno visibile, all'ulteriore distribuzione di tali informazioni.
5. L'ENISA coopera strettamente con gli Stati membri nella preparazione della relazione sulla situazione tecnica della cibersicurezza nell'Unione di cui al paragrafo 1, lettera e). La relazione è basata su informazioni pubblicamente disponibili, sull'analisi condotta dall'ENISA stessa e sulle relazioni condivise, tra l'altro, dai CSIRT degli Stati membri o dai punti di contatto unici istituiti dalla direttiva (UE) 2022/2555, in entrambi i casi su base volontaria, dall'EC3 e dal CERT-UE. D'intesa con i soggetti che hanno contribuito alla relazione, l'ENISA può rendere pubblicamente disponibile una versione aggregata della relazione.

Articolo 12 *Allerte precoci*

1. Le allerte precoci di cui all'articolo 11, paragrafo 1, primo comma, lettera b), del presente regolamento contengono informazioni pertinenti riguardanti un incidente significativo o su vasta scala, potenziale o in corso, o una minaccia informatica di potenziale natura transfrontaliera, in relazione ai settori elencati negli allegati I e II della direttiva (UE) 2022/2555. Tali informazioni possono includere vulnerabilità pubblicamente note e l'indicazione della possibilità che incidano su prodotti con elementi digitali disciplinati dal regolamento (UE) 2024/2847, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce e raccomandazioni sulle misure di attenuazione.
2. Le allerte precoci di cui all'articolo 11, paragrafo 1, primo comma, lettera b), sono inviate quanto prima ai CSIRT interessati e, se del caso, alla rete di CSIRT e a EU-CyCLONe.

3. L'ENISA offre un servizio di allerta precoce ai soggetti che operano nei settori elencati negli allegati I e II della direttiva (UE) 2022/2555.
4. Il servizio di cui al paragrafo 3 è fornito su richiesta del soggetto e in un formato leggibile da un dispositivo automatico messo a disposizione del pubblico. Tale servizio comprende la condivisione di informazioni sugli indicatori delle minacce informatiche e raccomandazioni sulle misure di attenuazione.
5. L'ENISA istituisce una procedura per diffondere le allerte precoci tra i soggetti di cui al paragrafo 3.

Articolo 13

Sostegno nella risposta agli incidenti e nel riesame degli stessi

1. L'ENISA gestisce e amministra, in tutto o in parte, la riserva dell'UE per la cibersicurezza, conformemente al regolamento (UE) 2025/38.
2. Su richiesta della Commissione o di EU-CyCLONe, l'ENISA, con il sostegno della rete di CSIRT e con l'approvazione dello Stato membro interessato, riesamina e valuta gli incidenti di cibersicurezza significativi o gli incidenti di cibersicurezza su vasta scala conformemente all'articolo 21 del regolamento (UE) 2025/38.
3. L'ENISA assiste, in cooperazione con Europol e i CSIRT o altre autorità competenti, a seconda dei casi, singoli soggetti essenziali e importanti, elencati negli allegati I e II della direttiva (UE) 2022/2555, nella preparazione e nella risposta agli incidenti di ransomware, e nella ripresa da tali incidenti. A tal fine, l'ENISA istituisce un helpdesk e, in particolare, si avvale della migliore conoscenza situazionale condivisa del panorama delle minacce e degli incidenti informatici a norma dell'articolo 11, paragrafo 1, primo comma, lettere a) e g), del presente regolamento.

Articolo 14

Esercitazioni di cibersicurezza a livello dell'Unione

1. L'ENISA assiste la Commissione nell'elaborazione di un programma continuo annuale di esercitazioni di cibersicurezza a livello dell'Unione.
2. L'ENISA mantiene un archivio degli insegnamenti tratti dalle esercitazioni di cui al paragrafo 1 e formula raccomandazioni rivolte agli Stati membri e, se del caso, ai soggetti dell'Unione in merito a come mettere in pratica in modo efficace ed efficiente tali insegnamenti.
3. Su richiesta di EU-CyCLONe o della Commissione, l'ENISA organizza o contribuisce all'organizzazione di esercitazioni di cibersicurezza a livello dell'Unione, compresa la verifica della preparazione a rispondere a incidenti e crisi di cibersicurezza su vasta scala a livello dell'Unione.
4. L'ENISA assiste gli Stati membri che lo richiedono nell'organizzazione di esercitazioni nazionali di cibersicurezza.
5. Su richiesta del CERT-UE, l'ENISA contribuisce all'organizzazione delle esercitazioni di cibersicurezza organizzate dal CERT-UE a norma dell'articolo 13, paragrafo 7, del regolamento (UE, Euratom) 2023/2841.

Articolo 15
Fornitura di strumenti e piattaforme

1. L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, comprese le piattaforme relative alla cibersecurity a livello dell'Unione, in particolare la piattaforma unica di segnalazione istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 [e il punto di accesso unico per la segnalazione degli incidenti istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555], nonché strumenti di prova a sostegno dell'attuazione delle procedure di valutazione della conformità a norma della pertinente normativa dell'Unione.
2. Ove opportuno, ai fini del paragrafo 1, l'ENISA coopera e scambia informazioni con la rete di CSIRT e, se del caso, con le autorità di vigilanza del mercato.

Articolo 16
Servizi di gestione delle vulnerabilità

L'ENISA sviluppa una capacità comune di servizi di gestione delle vulnerabilità dell'Unione e fornisce servizi di gestione delle vulnerabilità ai portatori di interessi:

- a) mantenendo la banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555;
- b) fornendo servizi di gestione delle vulnerabilità ai portatori di interessi, basandosi sulla banca dati europea delle vulnerabilità e utilizzando le informazioni pertinenti di cui dispone;
- c) se del caso, avviando una cooperazione strutturata con organizzazioni che forniscono programmi, registri o banche dati simili alla banca dati europea delle vulnerabilità;
- d) assistendo attivamente i CSIRT designati come coordinatori di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555 per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;
- e) sviluppando e mantenendo metodologie e meccanismi di governance per l'individuazione e la divulgazione coordinata delle vulnerabilità, in cooperazione con le autorità nazionali competenti, i CSIRT, l'industria e la comunità della ricerca.

Sezione 3

Certificazione della cibersecurity e normazione

Articolo 17
Certificazione della cibersecurity

1. L'ENISA favorisce e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersecurity di cui al titolo III del presente regolamento. L'ENISA è incaricata di:
 - a) preparare proposte di sistemi europei di certificazione della cibersecurity ("proposte di sistemi") per prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti e postura di cibersecurity dei soggetti conformemente

all'articolo 74 e, se del caso, elaborare specifiche tecniche conformemente all'articolo 77;

- b) mantenere i sistemi europei di certificazione della cibersecurity adottati conformemente all'articolo 75, in considerazione di un'eventuale revisione di tali sistemi a norma dell'articolo 76;
- c) promuovere la diffusione dei sistemi adottati e gestire un apposito sito web che fornisca informazioni sui sistemi europei di certificazione della cibersecurity, sui certificati europei di cibersecurity e sulle dichiarazioni UE di conformità, e li pubblicizza, conformemente all'articolo 79;
- d) organizzare lo sviluppo delle capacità relative ai processi di certificazione, alle attività di valutazione, alla revisione e alla valutazione tra pari, anche fornendo assistenza agli Stati membri, su loro richiesta, conformemente all'articolo 6, punto 12).

2. L'ENISA coadiuva la Commissione nelle attività seguenti:

- a) la governance dell'ECCG a norma dell'articolo 90;
- b) l'organizzazione di un'assemblea europea sulla certificazione della cibersecurity a norma dell'articolo 72, paragrafo 1;
- c) le attività relative al riconoscimento internazionale dei certificati europei di cibersecurity a norma dell'articolo 87;
- d) l'organizzazione di revisioni tra pari a norma dell'articolo 89;
- e) l'elaborazione di disposizioni tipo cui fare riferimento nei sistemi europei di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersecurity dei soggetti a norma dell'articolo 81, paragrafo 5.

Articolo 18

Normazione, specifiche tecniche e orientamenti

- 1. L'ENISA elabora specifiche tecniche e orientamenti a sostegno dell'attuazione della normativa dell'Unione nel settore della cibersecurity. Nell'elaborare tali specifiche tecniche, l'ENISA tiene conto delle norme europee e internazionali esistenti nonché di altre specifiche tecniche pertinenti. L'ENISA assicura la coerenza delle sue specifiche tecniche e dei suoi orientamenti.
- 2. L'ENISA monitora le attività di elaborazione della normazione a livello dell'Unione e, conformemente all'articolo 9, a livello internazionale, e vi partecipa, ove opportuno, anche assumendo un ruolo guida, al fine di sostenere le politiche dell'Unione in materia di cibersecurity.
- 3. L'ENISA contribuisce allo sviluppo e alla valutazione di algoritmi crittografici. Qualora un algoritmo crittografico sia valutato positivamente dall'ENISA, quest'ultima coopera, conformemente al regolamento (UE) n. 1025/2012, con gli organismi europei di normazione per contribuire alla sua normazione.
- 4. L'ENISA fornisce consulenza tecnica alla Commissione e, ove opportuno, agli Stati membri in merito a norme o specifiche tecniche adeguate a sostegno delle politiche dell'Unione in materia di cibersecurity, anche per quanto riguarda la normativa di armonizzazione dell'Unione nel settore della cibersecurity, in particolare il regolamento (UE) 2024/2847, i settori tecnici ai fini dell'articolo 25 della direttiva

(UE) 2022/2555 e i sistemi europei di certificazione della cibersecurity a norma dell'articolo 81, paragrafo 1, lettera d).

5. L'ENISA assiste la Commissione nella valutazione dei progetti di norme armonizzate a sostegno dell'attuazione della normativa di armonizzazione dell'Unione nel settore della cibersecurity.
6. L'ENISA promuove l'adozione di norme europee e internazionali in materia di cibersecurity.
7. L'ENISA svolge i compiti di cui ai paragrafi da 1 a 6 con integrità, imparzialità e riservatezza, anche ritirando o sospendendo la propria partecipazione a organismi tecnici specifici qualora quest'ultima sia in conflitto con altri compiti o obiettivi.

Sezione 4

Realizzazione dell'Accademia per le competenze in materia di cibersecurity

Articolo 19

Quadro europeo delle competenze in materia di cibersecurity

1. L'ENISA sviluppa e rende pubblicamente disponibile un quadro europeo delle competenze in materia di cibersecurity (*European Cybersecurity Skills framework*, "ECSF"). Prima di rendere l'ECSF pubblicamente disponibile o di aggiornarlo a norma del paragrafo 4, l'ENISA consulta la Commissione.
2. L'ECSF definisce i profili dei professionisti della cibersecurity e gli specifici compiti, competenze e conoscenze associati a un determinato profilo professionale. L'uso dell'ECSF da parte dei soggetti pubblici e privati ha carattere volontario.
3. L'ENISA può consultare i portatori di interessi per quanto riguarda lo sviluppo e l'adozione dell'ECSF.
4. L'ENISA valuta la necessità di aggiornare periodicamente l'ECSF e, ove opportuno, lo aggiorna.

Articolo 20

Sviluppo, adozione e mantenimento di sistemi europei di attestazione delle competenze individuali in materia di cibersecurity

1. L'ENISA sviluppa, adotta e mantiene sistemi europei di attestazione delle competenze individuali in materia di cibersecurity. L'uso di sistemi europei di attestazione delle competenze individuali in materia di cibersecurity è volontario per gli organismi pubblici nazionali e i soggetti privati, salvo diversamente specificato dal diritto nazionale.
2. Prima di avviare un nuovo sistema europeo di attestazione delle competenze individuali in materia di cibersecurity, l'ENISA consulta la Commissione. L'ENISA adotta tale sistema solo previo parere positivo della Commissione. Nella fase di elaborazione di un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity, l'ENISA può consultare i portatori di interessi pertinenti.
3. Un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity comprende quanto segue:

- a) l'oggetto e l'ambito di applicazione del sistema di attestazione sulla base dei profili professionali dell'ECSF o di loro sottoinsiemi;
 - b) i requisiti applicabili alle persone formate per effettuare le valutazioni ("valutatori") conformemente all'articolo 21, le competenze, le conoscenze e l'esperienza necessarie nonché i metodi di formazione;
 - c) l'analisi dell'adozione sul mercato, specifica per ciascun sistema di attestazione;
 - d) i risultati dell'apprendimento, i metodi di valutazione e le condizioni che i fornitori autorizzati di attestati utilizzano per valutare la dimostrazione, da parte dell'interessato, delle competenze richieste conformemente all'articolo 21;
 - e) ove opportuno, uno o più livelli di competenza;
 - f) le norme relative alla conservazione dei registri da parte dei fornitori autorizzati di attestati;
 - g) il contenuto e il formato degli attestati europei delle competenze individuali in materia di cibersecurity, tenendo debitamente conto dell'articolo 21, paragrafo 5, lettera e);
 - h) il periodo massimo di validità degli attestati europei delle competenze individuali in materia di cibersecurity rilasciati nell'ambito del sistema di attestazione.
4. Un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity può includere il costo indicativo di un attestato europeo delle competenze individuali in materia di cibersecurity.
 5. L'ENISA assicura una stretta cooperazione con gli Stati membri durante l'intera fase di preparazione dei sistemi europei di attestazione delle competenze individuali in materia di cibersecurity.
 6. La modifica di un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity non incide sull'autorizzazione concessa a norma dell'articolo 22, paragrafo 3, lettera a), che rimane valida per il periodo per il quale è concessa.

Articolo 21

Fornitori autorizzati di attestati

1. I fornitori autorizzati di attestati valutano se gli interessati soddisfano i requisiti di un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity e, qualora tali requisiti siano soddisfatti, rilasciano attestati europei delle competenze individuali in materia di cibersecurity. I fornitori autorizzati di attestati possono essere titolari di più autorizzazioni, ciascuna concessa per un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity.
2. L'ENISA fornisce orientamenti ai valutatori e impartisce loro una formazione obbligatoria in merito ai requisiti e ai metodi di valutazione previsti nel sistema europeo di attestazione delle competenze individuali in materia di cibersecurity di cui all'articolo 20, paragrafo 3, lettera b).
3. I soggetti che intendono diventare fornitori autorizzati di attestati o rinnovare la propria autorizzazione ("richiedenti") presentano una domanda all'ENISA. Essi soddisfano i requisiti seguenti:

- a) hanno personalità giuridica;
- b) sono in grado di svolgere i compiti stabiliti nel presente regolamento in relazione agli attestati europei delle competenze individuali in materia di cibersecurity, indipendentemente dal fatto che la valutazione sia effettuata dal fornitore autorizzato dell'attestato stesso o per suo conto e sotto la sua responsabilità;
- c) dispongono dei mezzi necessari per eseguire i compiti tecnici e amministrativi connessi al sistema europeo di attestazione delle competenze individuali in materia di cibersecurity in modo appropriato e hanno accesso a tutti gli strumenti e impianti necessari.

Ai fini del primo comma, lettera b), eventuali subappalti o consultazioni di personale esterno sono adeguatamente documentati, non prevedono alcun intermediario e sono oggetto di un accordo scritto che contempli, tra l'altro, la riservatezza e i conflitti di interessi.

4. I richiedenti non sono fornitori ad alto rischio.

5. I fornitori autorizzati di attestati rispettano gli obblighi seguenti:

- a) per l'attuazione di ciascun sistema europeo di attestazione delle competenze individuali in materia di cibersecurity:
 - i) dispongono dei valutatori e del personale necessari per svolgere in modo tempestivo le attività previste da tale sistema;
 - ii) garantiscono che i valutatori rispettino il segreto professionale, siano imparziali e svolgano il loro lavoro in modo indipendente e con la massima integrità professionale;
 - iii) dispongono di procedure scritte per lo svolgimento delle loro attività nell'ambito del sistema per il quale sono autorizzati;
- b) non valutano né rilasciano attestati europei delle competenze individuali in materia di cibersecurity ai propri valutatori;
- c) assicurano, ponendo in essere ove opportuno garanzie adeguate, che i loro valutatori possano svolgere il proprio lavoro in modo indipendente, in particolare qualora appartengano alla loro struttura o siano dipendenti o discendenti di tale struttura;
- d) non intraprendono attività alcuna che possa essere in conflitto con l'indipendenza di giudizio o l'integrità dei loro valutatori;
- e) provvedono affinché, su richiesta dell'interessato, gli attestati europei delle competenze individuali in materia di cibersecurity siano rilasciati sotto forma di attestati elettronici di attributi in un formato che può essere archiviato nei portafogli europei di identità digitale di cui al regolamento (UE) n. 910/2014.

6. I fornitori autorizzati di attestati informano immediatamente l'ENISA se uno dei requisiti di cui ai paragrafi 3 e 4 o gli obblighi di cui al paragrafo 5 non sono più soddisfatti o se sorgono dubbi in merito al fatto che tali requisiti o obblighi siano soddisfatti, anche per quanto riguarda l'indipendenza dei valutatori.

7. I fornitori autorizzati di attestati possono chiedere agli interessati il pagamento di diritti per la valutazione e il rilascio degli attestati europei delle competenze individuali in materia di cibersecurity, tenendo conto del costo indicativo di un

attestato europeo delle competenze individuali in materia di cibersicurezza di cui all'articolo 20, paragrafo 4, reso pubblico su un apposito sito web a norma dell'articolo 23, lettera d).

8. I richiedenti e i fornitori autorizzati di attestati consentono all'ENISA di effettuare valutazioni nell'ambito della procedura di domanda o del mantenimento dell'autorizzazione e di condividere tutte le informazioni pertinenti per far sì che i requisiti di cui ai paragrafi 3 e 4 o gli obblighi di cui al paragrafo 5 siano soddisfatti o continuino a essere soddisfatti conformemente all'articolo 22, paragrafo 2.

Articolo 22

Esame delle domande per diventare fornitore autorizzato di attestati e mantenimento delle autorizzazioni

1. I richiedenti versano un diritto all'ENISA per l'esame della loro domanda. I fornitori autorizzati di attestati versano un diritto all'ENISA per il mantenimento della loro autorizzazione.
2. L'ENISA valuta se i requisiti di cui all'articolo 21, paragrafi 3 e 4, e gli obblighi di cui all'articolo 21, paragrafo 5, sono soddisfatti o continuano a essere soddisfatti dai richiedenti e dai fornitori autorizzati di attestati.
3. Dopo aver esaminato una domanda alla luce dei requisiti di cui all'articolo 21, paragrafi 3 e 4, l'ENISA può adottare una delle decisioni seguenti:
 - a) concedere al richiedente lo status di fornitore autorizzato di attestati o il rinnovo di tale status;
 - b) respingere la domanda di diventare un fornitore autorizzato di attestati o di rinnovo dell'autorizzazione;
 - c) chiudere il processo d'esame della domanda a causa dell'inerzia del richiedente a seguito di una richiesta di ulteriori informazioni da parte dell'ENISA.

L'ENISA può modificare, sospendere o revocare tali decisioni sulla base della sua valutazione a norma dell'articolo 22, paragrafo 2, o nel caso di cui all'articolo 21, paragrafo 6.
4. L'ENISA adotta la decisione di cui al paragrafo 3 entro tre mesi dalla data di presentazione di una domanda conformemente all'articolo 21, paragrafo 3. Qualora abbia chiesto al richiedente ulteriori informazioni, l'ENISA adotta la decisione di cui al paragrafo 3 entro un mese dal ricevimento di tali ulteriori informazioni.
5. La decisione di cui al paragrafo 3, lettera a), ha una durata massima di tre anni e vi sono indicati i diritti dovuti per il mantenimento annuale dell'autorizzazione.
6. L'ENISA provvede affinché le sue attività relative allo sviluppo e all'adozione di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza di cui all'articolo 20 siano rigorosamente separate e svolte in modo indipendente dalle attività relative all'esame delle domande e alle valutazioni di cui ai paragrafi 2 e 3 del presente articolo.

Articolo 23

Informazione del pubblico

L'ENISA gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni pubbliche riguardanti:

- a) l'ECSF, comprendenti il quadro e il relativo calendario di aggiornamento;
- b) i sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza, i progressi compiuti e le tempistiche per il loro sviluppo;
- c) i diritti associati a ciascun sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza adottato a norma dell'articolo 47 del presente regolamento;
- d) il costo indicativo di un attestato europeo delle competenze individuali in materia di cibersicurezza a norma dell'articolo 20, paragrafo 4;
- e) l'elenco dei fornitori autorizzati di attestati.

Capo III **Organizzazione dell'ENISA**

Articolo 24 *Struttura amministrativa e di gestione dell'ENISA*

La struttura amministrativa e di gestione dell'ENISA è composta da:

- a) un consiglio di amministrazione, che esercita le funzioni di cui all'articolo 28;
- b) un comitato esecutivo, che esercita le funzioni di cui all'articolo 30;
- c) un direttore esecutivo, che esercita le competenze di cui all'articolo 32;
- d) un vicedirettore esecutivo, che esercita le competenze di cui all'articolo 34;
- e) un gruppo consultivo ENISA;
- f) una commissione di ricorso, che esercita le funzioni di cui agli articoli da 39 a 42.

Sezione 1 **Consiglio di amministrazione**

Articolo 25 *Composizione del consiglio di amministrazione*

1. Il consiglio di amministrazione è composto da un membro nominato da ciascuno Stato membro e due membri nominati dalla Commissione. Tutti i membri hanno diritto di voto.
2. Ciascun membro del consiglio di amministrazione ha un supplente. I supplenti rappresentano i membri in caso di assenza.
3. Ciascuno Stato membro nomina quale membro del consiglio di amministrazione la figura di vertice di un'autorità nazionale competente designata a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555. Qualora ciò non risulti fattibile, gli Stati membri nominano quale membro del consiglio di amministrazione un rappresentante di alto livello di un'autorità nazionale competente designata a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555.
4. I membri nominati dalla Commissione e i membri supplenti del consiglio di amministrazione sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle loro pertinenti abilità gestionali, amministrative e di bilancio. Per quanto riguarda i supplenti, la Commissione e gli Stati membri

mirano a conseguire una rappresentanza equilibrata di donne e uomini in seno al consiglio di amministrazione e si adoperano per limitarne l'avvicendamento al fine di garantire la continuità dei lavori del consiglio di amministrazione.

5. La durata del mandato dei membri nominati dagli Stati membri è pari alla durata del loro incarico di cui al paragrafo 3.
6. La durata del mandato dei supplenti e dei membri nominati dalla Commissione è di quattro anni. Il mandato è rinnovabile.

Articolo 26

Presidente del consiglio di amministrazione

1. Il consiglio di amministrazione elegge un presidente e un vicepresidente scegliendoli tra i suoi membri con diritto di voto. Il presidente e il vicepresidente sono eletti a maggioranza di due terzi dei membri del consiglio di amministrazione con diritto di voto.
2. Il vicepresidente sostituisce d'ufficio il presidente nel caso in cui quest'ultimo sia impossibilitato a svolgere i propri compiti.
3. Il mandato del presidente e del vicepresidente è di quattro anni e può essere rinnovato una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, quest'ultimo giunge automaticamente a termine alla stessa data.

Articolo 27

Riunioni del consiglio di amministrazione

1. Il presidente convoca le riunioni del consiglio di amministrazione.
2. Il direttore esecutivo partecipa alle riunioni del consiglio di amministrazione, senza diritto di voto.
3. Il consiglio di amministrazione tiene almeno due riunioni ordinarie l'anno. Si riunisce inoltre su istanza del presidente, su richiesta della Commissione o su richiesta di almeno un terzo dei suoi membri.
4. Un rappresentante del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca istituito dal regolamento (UE) 2021/887 è un osservatore permanente, senza diritto di voto, alle riunioni del consiglio di amministrazione.
5. Il consiglio di amministrazione può invitare a partecipare a una riunione, o a una parte di una riunione, in veste di osservatore ad hoc senza diritto di voto, qualsiasi persona il cui parere possa essere rilevante, fatte salve le disposizioni del regolamento interno del consiglio di amministrazione.
6. Alle riunioni del consiglio di amministrazione, i membri del consiglio di amministrazione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno del consiglio di amministrazione.

Articolo 28

Funzioni del consiglio di amministrazione

1. Il consiglio di amministrazione:

- a) stabilisce gli orientamenti generali del funzionamento dell'ENISA e assicura che essa operi secondo le regole e i principi stabiliti dal presente regolamento; assicura inoltre la coerenza del lavoro dell'ENISA con le attività svolte dagli Stati membri e a livello di Unione;
- b) adotta il progetto di documento unico di programmazione dell'ENISA di cui all'articolo 44 prima che sia trasmesso alla Commissione per parere;
- c) tenendo conto del parere della Commissione, adotta il documento unico di programmazione dell'ENISA conformemente all'articolo 29, paragrafo 2, lettera a);
- d) vigila sull'attuazione del programma annuale e pluriennale contenuto nel documento unico di programmazione;
- e) adotta il bilancio annuale dell'ENISA, conformemente all'articolo 29, paragrafo 2, lettera b), ed esercita altre funzioni in relazione al bilancio dell'ENISA a norma del capo IV;
- f) valuta e adotta la relazione annuale consolidata sulle attività dell'ENISA, inclusi i conti e una descrizione di come l'ENISA ha conseguito i propri indicatori di risultato, trasmette, entro il 1° luglio dell'anno successivo, sia la relazione annuale che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti; rende pubblica la relazione annuale;
- g) adotta la regolamentazione finanziaria applicabile all'ENISA conformemente all'articolo 50;
- h) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;
- i) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti da relazioni di revisione contabile e valutazioni interne ed esterne e dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalla Procura europea (EPPO);
- j) adotta il proprio regolamento interno, comprese regole per le decisioni provvisorie sulla delega di compiti specifici, a norma dell'articolo 30, paragrafo 7;
- k) in conformità del paragrafo 2 del presente articolo, esercita nei confronti del personale dell'ENISA i poteri conferiti dallo statuto dei funzionari dell'Unione europea ("statuto dei funzionari") e dal regime applicabile agli altri agenti dell'Unione europea ("regime applicabile agli altri agenti"), stabiliti nel regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio⁷³, rispettivamente all'autorità che ha il potere di nomina e all'autorità abilitata a concludere i contratti di assunzione ("poteri dell'autorità che ha il potere di nomina");
- l) adotta disposizioni di attuazione per dare effetto allo statuto dei funzionari e al regime applicabile agli altri agenti a norma dell'articolo 110, paragrafo 2, dello statuto dei funzionari;

⁷³

GU L 56 del 4.3.1968, pag. 1, ELI: [http://data.europa.eu/eli/reg/1968/259\(1\)/oj](http://data.europa.eu/eli/reg/1968/259(1)/oj).

- m) nomina il direttore esecutivo e, qualora decida di creare la funzione di vicedirettore esecutivo, il vicedirettore esecutivo e, se del caso, ne proroga il mandato o li rimuove dall'incarico a norma dell'articolo 31;
 - n) nomina un contabile, soggetto allo statuto dei funzionari e al regime applicabile agli altri agenti, che è indipendente nell'esercizio delle sue funzioni;
 - o) prende tutte le decisioni sull'istituzione delle strutture interne dell'ENISA e, se necessario, sulla relativa modifica, in considerazione delle necessità per l'attività dell'ENISA e secondo una gestione di bilancio sana;
 - p) autorizza la conclusione di accordi di lavoro in relazione all'articolo 68;
 - q) autorizza la conclusione di accordi di lavoro conformemente all'articolo 70;
 - r) nomina i membri della commissione di ricorso e li rimuove dall'incarico a norma dell'articolo 29, paragrafo 2, lettera d);
 - s) adotta regole per la prevenzione e la gestione dei conflitti di interesse in relazione ai membri della commissione di ricorso.
2. In conformità dell'articolo 110, paragrafo 2, dello statuto dei funzionari, il consiglio di amministrazione adotta una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i pertinenti poteri di autorità che ha il potere di nomina e definisce le condizioni di sospensione della delega di poteri. Il direttore esecutivo può subdelegare tali poteri.
3. Qualora circostanze eccezionali lo richiedano, il consiglio di amministrazione può adottare una decisione per sospendere temporaneamente la delega al direttore esecutivo dei poteri di autorità che ha il potere di nomina e tutti i poteri di autorità che ha il potere di nomina che il direttore esecutivo abbia subdelegato ed esercitarli esso stesso o delegarli a uno dei suoi membri o a un membro del personale diverso dal direttore esecutivo.

Articolo 29

Modalità di voto del consiglio di amministrazione

1. Salvo disposizione contraria del presente regolamento, il consiglio di amministrazione adotta le proprie decisioni a maggioranza assoluta dei suoi membri con diritto di voto.
2. La maggioranza di due terzi dei membri del consiglio di amministrazione con diritto di voto è necessaria per:
 - a) l'adozione del documento unico di programmazione di cui all'articolo 28, paragrafo 1, lettera c);
 - b) l'adozione del bilancio annuale di cui all'articolo 28, paragrafo 1, lettera e);
 - c) la nomina del direttore esecutivo e del vicedirettore esecutivo, la proroga del loro mandato o la loro rimozione dall'incarico a norma degli articoli 31 e 33;
 - d) la nomina dei membri della commissione di ricorso e la loro rimozione dall'incarico a norma dell'articolo 36.
3. Le decisioni riguardanti questioni relative al bilancio o alle risorse umane, in particolare quelle di cui all'articolo 28, paragrafo 1, lettere c), e), f), g), h), i), k), l), m) e n), sono adottate solo se i rappresentanti della Commissione esprimono un voto

favorevole. Ai fini dell'adozione delle decisioni di cui all'articolo 28, paragrafo 1, lettera c), relative al documento unico di programmazione dell'ENISA, il voto favorevole del rappresentante della Commissione è richiesto soltanto per gli elementi della decisione non correlati al programma di lavoro annuale e pluriennale dell'ENISA.

4. Ogni membro con diritto di voto dispone di un voto. In assenza di un membro con diritto di voto, il supplente è abilitato a esercitare il diritto di voto del membro.
5. Il presidente del consiglio di amministrazione partecipa al voto.
6. Il direttore esecutivo non partecipa al voto.
7. Il regolamento interno del consiglio di amministrazione stabilisce le regole dettagliate concernenti la votazione, in particolare le circostanze in cui un membro può agire per conto di un altro.

Sezione 2

Comitato esecutivo

Articolo 30

Comitato esecutivo

1. Il consiglio di amministrazione è assistito da un comitato esecutivo.
2. Il comitato esecutivo:
 - a) prepara le decisioni che dovranno essere adottate dal consiglio di amministrazione;
 - b) insieme al consiglio di amministrazione, garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti da relazioni di revisione contabile e valutazioni interne ed esterne e dalle indagini svolte dall'OLAF e dall'EPPO;
 - c) fatte salve le responsabilità del direttore esecutivo stabilite all'articolo 32, fornisce assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione, al fine di rafforzare il controllo della gestione amministrativa e di bilancio.
3. Il comitato esecutivo è composto dal presidente del consiglio di amministrazione, da un rappresentante della Commissione nel consiglio di amministrazione e da altri tre membri nominati dal consiglio di amministrazione tra i suoi membri aventi diritto di voto. Il presidente del consiglio di amministrazione è anche presidente del comitato esecutivo. Le nomine dei membri del comitato esecutivo mirano ad assicurare l'equilibrio di genere nel comitato esecutivo. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.
4. La durata del mandato dei membri del comitato esecutivo è di quattro anni. Il mandato è rinnovabile. La durata del mandato dei membri del comitato esecutivo coincide con la durata del loro mandato come membri del consiglio di amministrazione.
5. Il comitato esecutivo tiene almeno una riunione ordinaria ogni tre mesi. Si riunisce inoltre su istanza del presidente o su richiesta dei suoi membri.
6. Il consiglio di amministrazione stabilisce il regolamento interno del comitato esecutivo.

7. Se necessario per ragioni di urgenza, il comitato esecutivo può prendere determinate decisioni provvisorie a nome del consiglio di amministrazione, in particolare su questioni di gestione amministrativa, tra cui la sospensione della delega dei poteri dell'autorità che ha il potere di nomina e le questioni di bilancio. Tali decisioni provvisorie sono notificate al consiglio di amministrazione senza indebito ritardo. Il consiglio di amministrazione decide poi se approvare o rigettare la decisione provvisoria entro tre mesi dalla sua adozione. Il comitato esecutivo non adotta per conto del consiglio di amministrazione decisioni che richiedono l'approvazione di una maggioranza di due terzi dei membri del consiglio di amministrazione con diritto di voto.

Sezione 3 **Direttore esecutivo**

Articolo 31

Nomina, rimozione dall'incarico e proroga del mandato

1. Il direttore esecutivo è nominato dal consiglio di amministrazione in base al merito e alle competenze, a partire da un elenco di candidati proposto dalla Commissione, secondo una procedura di selezione aperta e trasparente.
2. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione è invitato a fare una dichiarazione dinanzi alla commissione competente del Parlamento europeo e a rispondere alle domande dei deputati.
3. Il direttore esecutivo è assunto in qualità di agente temporaneo dell'ENISA ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.
4. Ai fini della conclusione del contratto con il direttore esecutivo, l'ENISA è rappresentata dal presidente del consiglio di amministrazione.
5. La durata del mandato del direttore esecutivo è di cinque anni. In tempo utile prima della fine di tale periodo, la Commissione esegue una valutazione che tiene conto dell'operato del direttore esecutivo e dei compiti e delle sfide futuri dell'ENISA.
6. Su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di amministrazione può prorogare il mandato del direttore esecutivo una sola volta, per un massimo di cinque anni.
7. Il direttore esecutivo il cui mandato sia stato prorogato non può partecipare a un'altra procedura di selezione per lo stesso posto alla fine del periodo complessivo.
8. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo a norma del paragrafo 6. Entro i tre mesi che precedono tale proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.
9. Il direttore esecutivo può essere rimosso dall'incarico solo su decisione del consiglio di amministrazione, su proposta della Commissione.

Articolo 32

Compiti e responsabilità del direttore esecutivo

1. Il direttore esecutivo gestisce l'ENISA e risponde al consiglio di amministrazione.

2. Il direttore esecutivo è indipendente nello svolgimento dei suoi compiti e non sollecita né accetta istruzioni da alcun governo o altro organismo.
3. Il direttore esecutivo riferisce al Parlamento europeo sullo svolgimento dei suoi compiti, se invitato a farlo. Il Consiglio può invitare il direttore esecutivo a riferire sullo svolgimento dei suoi compiti.
4. Il direttore esecutivo è il rappresentante legale dell'ENISA.
5. Il direttore esecutivo è responsabile dell'esecuzione dei compiti assegnati all'ENISA dal presente regolamento. In particolare:
 - a) provvede all'amministrazione corrente dell'ENISA;
 - b) attua le decisioni adottate dal consiglio di amministrazione;
 - c) garantisce il rispetto della regolamentazione finanziaria dell'ENISA;
 - d) prepara il progetto di documento unico di programmazione e lo presenta al consiglio di amministrazione per approvazione prima di trasmetterlo alla Commissione per parere;
 - e) attua il documento unico di programmazione e riferisce al consiglio di amministrazione in merito alla sua attuazione;
 - f) elabora la relazione annuale consolidata sulle attività dell'ENISA, compresa l'attuazione del suo programma di lavoro annuale, e la presenta al consiglio di amministrazione per valutazione e adozione;
 - g) predispone un piano d'azione che dia seguito alle conclusioni delle valutazioni retrospettive dell'ENISA di cui all'articolo 121 e riferisce ogni due anni alla Commissione sui progressi compiuti;
 - h) predispone un piano d'azione che dia seguito alle conclusioni delle relazioni di revisione contabile e delle valutazioni interne ed esterne, come pure delle indagini svolte dall'OLAF e dall'EPPO, e riferisce ogni due anni alla Commissione e periodicamente al consiglio di amministrazione in merito ai progressi compiuti;
 - i) predispone il progetto della regolamentazione finanziaria applicabile all'ENISA di cui all'articolo 50;
 - j) predispone il progetto di stato di previsione delle entrate e delle spese dell'ENISA e l'esecuzione del bilancio;
 - k) protegge gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, fatti salvi i poteri investigativi dell'OLAF e dell'EPPO, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, ove opportuno, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive;
 - l) elabora per l'ENISA una strategia antifrode, una strategia per conseguire miglioramenti dell'efficienza e realizzare sinergie, una strategia di cooperazione con i paesi terzi o le organizzazioni internazionali e una strategia per la gestione organizzativa e i sistemi di controllo interno e le presenta al consiglio di amministrazione per approvazione;

- m) sviluppa e mantiene i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con i pertinenti portatori di interessi;
 - n) scambia periodicamente opinioni e informazioni con i pertinenti soggetti dell'Unione riguardo alle loro attività in materia di cibersecurity, al fine di garantire la coerenza nell'attuazione della politica dell'Unione in tale settore;
 - o) promuove la diversità e l'equilibrio di genere nell'assunzione del personale dell'ENISA;
 - p) adotta sistemi europei di attestazione delle competenze individuali in materia di cibersecurity a norma dell'articolo 20, paragrafo 1;
 - q) adotta decisioni nei confronti dei richiedenti che presentano domanda per diventare fornitori autorizzati di attestati o per rinnovare la propria autorizzazione, a norma dell'articolo 22, paragrafo 3;
 - r) svolge gli altri compiti attribuiti al direttore esecutivo dal presente regolamento.
6. In base alle esigenze e nell'ambito degli obiettivi e dei compiti dell'ENISA, il direttore esecutivo può istituire gruppi di lavoro ad hoc composti da esperti, anche esperti inviati dalle autorità competenti degli Stati membri. Il direttore esecutivo ne informa il consiglio di amministrazione in anticipo. Le procedure relative in particolare alla composizione dei gruppi di lavoro, alla nomina degli esperti dei gruppi di lavoro da parte del direttore esecutivo e al funzionamento dei gruppi di lavoro sono specificate nel regolamento interno dell'ENISA.
7. Se necessario per svolgere i compiti dell'ENISA in maniera efficiente ed efficace e in base a un'adeguata analisi costi-benefici, il direttore esecutivo può decidere di istituire uno o più uffici locali in uno o più Stati membri. Prima di decidere di istituire un ufficio locale, il direttore esecutivo chiede il parere degli Stati membri interessati, compreso lo Stato membro che ospita la sede dell'ENISA, e ottiene il previo consenso della Commissione e del consiglio di amministrazione. In caso di disaccordo durante il processo di consultazione tra il direttore esecutivo e gli Stati membri interessati, la questione è sottoposta all'esame del Consiglio. Il numero complessivo dei membri del personale in tutti gli uffici locali è ridotto al minimo e non supera il 40 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede. Il numero dei membri del personale in ciascuno degli uffici locali non supera il 10 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede.
8. La decisione di istituire un ufficio locale precisa la gamma di attività che devono essere espletate presso l'ufficio locale al fine di evitare costi inutili e duplicazioni di funzioni amministrative dell'ENISA.

Sezione 4

Vicedirettore esecutivo

Articolo 33
Vicedirettore esecutivo

1. Il consiglio di amministrazione può decidere di creare una funzione di vicedirettore esecutivo per assistere il direttore esecutivo.
2. Qualora il consiglio di amministrazione decida di creare una funzione di vicedirettore esecutivo, le disposizioni dell'articolo 31 si applicano di conseguenza al vicedirettore esecutivo.

Articolo 34
Compiti e responsabilità del vicedirettore esecutivo

Il vicedirettore esecutivo assiste il direttore esecutivo nella gestione dell'ENISA e nello svolgimento dei compiti di cui all'articolo 32. In caso di assenza o indisponibilità del direttore esecutivo, o se il posto è vacante, il vicedirettore esecutivo ne fa le veci durante il periodo di assenza o fino alla copertura del posto.

Sezione 5
Gruppo consultivo ENISA

Articolo 35
Gruppo consultivo ENISA

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce in maniera trasparente il gruppo consultivo ENISA. Il gruppo consultivo ENISA è composto da esperti riconosciuti che rappresentano i pertinenti portatori di interessi, quali il settore della cibersecurity, il settore delle TIC, le PMI, i soggetti che operano nei settori elencati negli allegati I e II della direttiva (UE) 2022/2555, i fabbricanti di prodotti con elementi digitali e i gestori di software open source ai sensi del regolamento (UE) 2024/2847, gli organismi di valutazione della conformità notificati nell'ambito del quadro europeo di certificazione della cibersecurity di cui all'articolo 93 e al regolamento (UE) 2024/2847, i soggetti che operano nel settore dei mezzi di identificazione elettronica, le organizzazioni dei consumatori, gli esperti del mondo accademico nel settore della cibersecurity, le organizzazioni europee di normazione, nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati. Tali esperti riconosciuti sono cittadini degli Stati membri. Il consiglio di amministrazione si adopera per garantire un opportuno equilibrio geografico e di genere, nonché un equilibrio tra i diversi gruppi di portatori di interessi.
2. Le procedure per il gruppo consultivo ENISA, in particolare per quanto riguarda la composizione, la proposta del direttore esecutivo di cui al paragrafo 1, il numero e la nomina dei membri e il funzionamento del gruppo consultivo ENISA, sono specificati nel regolamento interno dell'ENISA e resi pubblici.
3. Il gruppo consultivo ENISA è presieduto dal direttore esecutivo o da qualsiasi altra persona nominata dal direttore esecutivo caso per caso.
4. La durata del mandato dei membri del gruppo consultivo ENISA è di due anni e mezzo ed è rinnovabile una volta. I membri del consiglio di amministrazione non possono essere membri del gruppo consultivo ENISA. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare alle riunioni del gruppo

consultivo ENISA e a partecipare alle sue attività. Il direttore esecutivo può invitare a partecipare alle riunioni del gruppo consultivo ENISA e alle sue attività i rappresentanti di altri organismi che non siano membri di tale gruppo.

5. Il gruppo consultivo ENISA fornisce consulenza all'ENISA relativamente allo svolgimento dei suoi compiti, tranne per quanto concerne l'applicazione delle disposizioni dei titoli III, IV e V del presente regolamento. In particolare, esso consiglia il direttore esecutivo ai fini della stesura di una proposta relativa al programma di lavoro annuale dell'ENISA e della comunicazione con i relativi portatori di interessi sulle questioni inerenti al programma di lavoro annuale.
6. Il gruppo consultivo ENISA informa periodicamente il consiglio di amministrazione sulle sue attività.
7. L'ENISA fornisce il supporto logistico necessario al gruppo consultivo ENISA e provvede alle funzioni di segretariato per le sue riunioni.

Sezione 6

Commissione di ricorso

Articolo 36

Istituzione e composizione della commissione di ricorso

1. L'ENISA istituisce una commissione di ricorso con decisione del consiglio di amministrazione.
2. La commissione di ricorso è composta da un presidente e da altri tre membri. Ciascun membro della commissione di ricorso ha un supplente. Il supplente rappresenta il membro in caso di assenza di quest'ultimo.
3. Il consiglio di amministrazione nomina il presidente, gli altri membri e i loro supplenti in base a un elenco di candidati idonei predisposto dalla Commissione. L'elenco dei candidati idonei è valido per un periodo di quattro anni. La validità di tale elenco può essere prorogata dal consiglio di amministrazione per ulteriori periodi di quattro anni su proposta della Commissione.
4. Qualora ne ravvisi la necessità per la natura stessa del ricorso, la commissione di ricorso può chiedere al consiglio di amministrazione di nominare due ulteriori membri e i relativi supplenti sulla base dell'elenco di cui al paragrafo 3.
5. La commissione di ricorso adotta e pubblica il proprio regolamento interno.

Articolo 37

Membri della commissione di ricorso

1. La durata del mandato dei membri della commissione di ricorso e dei loro supplenti è di quattro anni. Il mandato può essere rinnovato dal consiglio di amministrazione per ulteriori periodi di quattro anni su proposta della Commissione.
2. I membri della commissione di ricorso sono indipendenti e non svolgono altri compiti in seno all'ENISA. Nelle loro decisioni non sollecitano né accettano istruzioni da alcun governo o altro organismo né da soggetti privati.

3. Durante il loro mandato i membri della commissione di ricorso possono essere rimossi dall'incarico o dall'elenco dei candidati idonei solo per gravi motivi e se il consiglio di amministrazione decide in tal senso su proposta della Commissione.

Articolo 38

Esclusione e ricazione

1. I membri della commissione di ricorso non partecipano al procedimento di ricorso se vi hanno un interesse personale, se vi sono precedentemente intervenuti in veste di rappresentanti di una delle parti o se hanno partecipato all'adozione della decisione impugnata.
2. Se, per uno dei motivi di cui al paragrafo 1 o per qualsivoglia altro motivo, un membro della commissione di ricorso ritiene di doversi astenere dal partecipare a un procedimento di ricorso, ne informa la commissione stessa.
3. Qualsiasi membro della commissione di ricorso può essere ricasato da una delle parti del procedimento per uno dei motivi elencati al paragrafo 1 oppure per sospetta parzialità. La ricazione non è ammessa qualora detta parte del procedimento di ricorso abbia compiuto atti procedurali pur essendo a conoscenza di un motivo di ricazione. La ricazione non può essere fondata sulla nazionalità dei membri della commissione di ricorso.
4. Nei casi di cui ai paragrafi 2 e 3, la commissione di ricorso decide come procedere senza la partecipazione del membro interessato. Ai fini della decisione, il membro interessato è sostituito nella commissione di ricorso dal suo supplente.

Articolo 39

Ricorsi contro le decisioni e ricorsi per carenza

1. Un ricorso può essere presentato dinanzi la commissione di ricorso:
 - a) avverso le decisioni adottate dall'ENISA a norma dell'articolo 22, paragrafo 3;
 - b) per mancata azione da parte dell'ENISA entro i termini applicabili di cui all'articolo 22, paragrafo 4.
2. Il ricorso presentato a norma del paragrafo 1 è oggetto di una revisione precontenziosa conformemente all'articolo 41 prima di essere sottoposto all'esame della commissione di ricorso.
3. Un ricorso presentato a norma del paragrafo 1 non ha effetto sospensivo.

Articolo 40

Legittimazione a presentare ricorso, termini e forma

1. I richiedenti ai sensi dell'articolo 21, paragrafo 3, possono presentare ricorso
 - a) avverso una decisione dell'ENISA nei loro confronti a norma dell'articolo 22, paragrafo 3;
 - b) per mancata azione da parte dell'ENISA entro i termini applicabili di cui all'articolo 22, paragrafo 4, relativamente a una domanda da essi presentata all'ENISA.
2. Nel caso di cui al paragrafo 1, lettera a), il ricorso, insieme a una memoria che ne precisi i motivi, è presentato per iscritto conformemente al regolamento interno di cui

all'articolo 36, paragrafo 5, entro due mesi dalla notifica della decisione al richiedente interessato o, in assenza di tale notifica, dal giorno in cui il richiedente è venuto a conoscenza della decisione.

3. Nel caso di cui al paragrafo 1, lettera b), il ricorso è presentato all'ENISA per iscritto conformemente al regolamento interno di cui all'articolo 36, paragrafo 5, entro due mesi dal giorno della scadenza del termine di cui all'articolo 22, paragrafo 4.

Articolo 41

Revisione precontenziosa

1. Qualora ritenga che il ricorso sia ammissibile e fondato, l'ENISA rettifica la decisione o mancata azione di cui all'articolo 40, paragrafo 1.
2. Qualora non rettifichi la decisione entro un mese dal ricevimento del ricorso, l'ENISA decide immediatamente se sospendere l'applicazione della sua decisione e deferisce il ricorso in oggetto alla commissione di ricorso.

Articolo 42

Esame delle decisioni sui ricorsi

1. La commissione di ricorso decide se accogliere o respingere il ricorso entro tre mesi dalla sua presentazione. Nell'esame di un ricorso, la commissione di ricorso agisce entro i termini stabiliti nel proprio regolamento interno. Ogniqualvolta sia necessario, invita le parti del procedimento di ricorso a presentare, entro un dato termine, osservazioni sulle sue notifiche o sulle comunicazioni effettuate dalle altre parti del procedimento di ricorso. Le parti del procedimento di ricorso possono presentare osservazioni orali.
2. Se constata la fondatezza dei motivi del ricorso, la commissione di ricorso rinvia il caso all'ENISA. Quest'ultima adotta la decisione definitiva conformemente alle conclusioni della commissione di ricorso e fornisce una motivazione. L'ENISA informa di conseguenza le parti del procedimento di ricorso.

Articolo 43

Azione dinanzi alla Corte di giustizia dell'Unione europea

1. È possibile presentare alla Corte di giustizia dell'Unione europea ricorsi diretti all'annullamento di decisioni dell'ENISA adottate a norma dell'articolo 22, paragrafo 3, o ricorsi per carenza entro i termini applicabili a norma dell'articolo 22, paragrafo 4, dopo che sia stata esperita la procedura di ricorso all'interno dell'ENISA di cui agli articoli da 39 a 42 o in caso di mancata azione entro il termine applicabile a norma dell'articolo 41, paragrafo 2.
2. L'ENISA adotta tutti i provvedimenti necessari per conformarsi alla sentenza della Corte di giustizia dell'Unione europea.

Sezione 7

Funzionamento

Articolo 44
Documento unico di programmazione

1. L'ENISA opera conformemente a un documento unico di programmazione contenente il programma di lavoro annuale e pluriennale, che include tutte le attività pianificate.
2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti dalla Commissione, predispone un progetto di documento unico di programmazione, di cui al paragrafo 1, con la corrispondente pianificazione delle risorse finanziarie e umane, conformemente all'articolo 32 del regolamento delegato (UE) 2019/715 della Commissione⁷⁴.
3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1, tenendo conto del parere della Commissione di cui all'articolo 32, paragrafo 7, del regolamento delegato (UE) 2019/715. Qualora decida di non tener conto di un elemento del parere della Commissione, il consiglio di amministrazione fornisce una giustificazione dettagliata per tale decisione. Il consiglio di amministrazione trasmette il documento unico di programmazione al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, unitamente a eventuali successive versioni aggiornate di tale documento.
4. Il documento unico di programmazione diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione ed è adeguato secondo necessità.
5. Il programma di lavoro annuale comprende gli obiettivi dettagliati e i risultati attesi, compresi gli indicatori di risultato. Esso contiene inoltre una descrizione delle azioni da finanziare e un'indicazione delle risorse finanziarie e umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio per attività e gestione per attività. Il programma di lavoro annuale è coerente con il programma di lavoro pluriennale di cui al paragrafo 7. Indica chiaramente i compiti aggiunti, modificati o soppressi rispetto all'esercizio finanziario precedente.
6. Quando all'ENISA è assegnato un nuovo compito, il consiglio di amministrazione modifica il programma di lavoro annuale adottato. Le modifiche sostanziali del programma di lavoro annuale sono adottate con la stessa procedura di quella applicabile al programma di lavoro annuale iniziale. Il consiglio di amministrazione può delegare al direttore esecutivo il potere di apportare modifiche non sostanziali al programma di lavoro annuale.
7. Il programma di lavoro pluriennale definisce la programmazione strategica generale, compresi gli obiettivi, i risultati attesi e gli indicatori di prestazione. Riporta inoltre la programmazione delle risorse, compresi il bilancio pluriennale e il personale.
8. La programmazione delle risorse è aggiornata ogni anno. La programmazione strategica è aggiornata secondo necessità, in particolare per adattarla all'esito della valutazione di cui all'articolo 120.

⁷⁴ Regolamento delegato (UE) 2019/715 della Commissione, del 18 dicembre 2018, relativo al regolamento finanziario quadro degli organismi istituiti in virtù del TFUE e del trattato Euratom, di cui all'articolo 70 del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio (GU L 122 del 10.5.2019, pag. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

Capo IV
Formazione e struttura del bilancio dell'ENISA

Articolo 45
Formazione del bilancio dell'ENISA

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione provvisorio delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo, comprendente la tabella dell'organico, e lo trasmette al consiglio di amministrazione.
2. Il progetto di stato di previsione provvisorio si basa sugli obiettivi e sui risultati attesi del programma di lavoro annuale e tiene conto delle risorse finanziarie necessarie per conseguire tali obiettivi e risultati attesi, conformemente al principio della sana gestione finanziaria e performance.
3. Sulla base del progetto di stato di previsione provvisorio, il consiglio di amministrazione adotta un progetto di stato di previsione delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo e lo trasmette alla Commissione entro il 31 gennaio di ogni anno.
4. La Commissione trasmette il progetto di stato di previsione all'autorità di bilancio insieme al progetto di bilancio generale dell'Unione. Il progetto di stato di previsione è altresì messo a disposizione dell'ENISA.
5. Sulla base dello stato di previsione, la Commissione iscrive le stime che ritiene necessarie, per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale dell'Unione, nel progetto di bilancio generale dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente agli articoli 313 e 314 TFUE.
6. L'autorità di bilancio autorizza gli stanziamenti a titolo di contributo del bilancio generale dell'Unione destinato all'ENISA.
7. L'autorità di bilancio adotta la tabella dell'organico dell'ENISA.
8. Il consiglio di amministrazione adotta il bilancio dell'ENISA. Il bilancio diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione e, se necessario, è adeguato di conseguenza.
9. Per qualsiasi progetto di natura immobiliare che possa avere implicazioni significative per il bilancio dell'ENISA si applica il regolamento delegato (UE) 2019/715.

Articolo 46
Struttura del bilancio dell'ENISA

1. Tutte le entrate e le spese dell'ENISA sono oggetto di previsioni per ciascun esercizio finanziario e sono iscritte nel bilancio dell'ENISA. L'esercizio finanziario corrisponde all'anno civile.
2. Le entrate e le spese iscritte nel bilancio dell'ENISA devono essere in pareggio.
3. Fatte salve altre risorse, le entrate dell'ENISA comprendono:
 - a) un contributo dell'Unione iscritto al bilancio generale dell'Unione;
 - b) entrate con destinazione specifica volte a finanziare spese specifiche conformemente alla regolamentazione finanziaria di cui all'articolo 50;

- c) finanziamenti dell'Unione sotto forma di accordi di contributo o di sovvenzioni ad hoc secondo la regolamentazione finanziaria dell'ENISA di cui all'articolo 50 e le disposizioni dei pertinenti strumenti di sostegno alle politiche dell'Unione;
 - d) i diritti riscossi presso i richiedenti per le attività connesse ai sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza di cui all'articolo 22, paragrafo 1;
 - e) i diritti riscossi presso gli organismi di valutazione della conformità per la partecipazione a un sistema europeo di certificazione della cibersicurezza e il rilascio di certificati europei di cibersicurezza nell'ambito di detto sistema, come prescritto all'articolo 47, paragrafo 2;
 - f) i diritti riscossi presso autorità pubbliche o organismi privati in relazione a strumenti di prova a norma dell'articolo 47, paragrafo 3;
 - g) eventuali contributi dei paesi terzi che partecipano ai lavori dell'ENISA a norma dell'articolo 70, paragrafo 4;
 - h) eventuali contributi volontari degli Stati membri, in denaro o in natura.
4. Gli Stati membri che versano contributi volontari a norma del paragrafo 3, lettera g), non possono rivendicare alcun diritto o servizio specifico per effetto di tale contributo.
5. Le spese dell'ENISA comprendono le retribuzioni del personale, le spese amministrative e di infrastruttura e le spese operative.

Articolo 47

Diritti

1. In relazione a ciascuna attività nell'ambito del sistema europeo di attestazione di cui all'articolo 22, paragrafo 1, i seguenti diritti sono riscossi presso i richiedenti ai sensi dell'articolo 21, paragrafo 3, o presso i fornitori autorizzati di attestati, per contribuire a coprire integralmente i costi delle attività svolte dall'ENISA:
- a) rilascio di autorizzazioni in seguito all'esame dei requisiti di cui all'articolo 21, paragrafi 3 e 4, compresa l'esecuzione di valutazioni;
 - b) mantenimento annuale dell'autorizzazione;
 - c) rinnovo delle autorizzazioni per i fornitori di attestati europei delle competenze individuali in materia di cibersicurezza, compresa l'esecuzione di valutazioni.
2. In relazione alla certificazione, i seguenti diritti sono riscossi presso gli organismi di valutazione della conformità per il mantenimento dei sistemi europei di certificazione della cibersicurezza nell'ambito dei quali sono rilasciati i certificati europei di cibersicurezza, in particolare:
- a) un diritto annuale per la partecipazione a un sistema europeo di certificazione della cibersicurezza;
 - b) un diritto per il rilascio dei certificati europei di cibersicurezza nell'ambito dei sistemi europei di certificazione della cibersicurezza.

I diritti di cui alla lettera b) sono riscossi quando l'organismo di valutazione della conformità trasmette i certificati europei di cibersicurezza all'ENISA ai fini della pubblicazione sul sito web di quest'ultima a norma dell'articolo 79.

3. In relazione agli strumenti di prova di cui all'articolo 15, paragrafo 1, per il loro utilizzo è riscosso un diritto presso qualsiasi autorità pubblica o organismo privato.
4. I diritti sono espressi e riscossi in euro.
5. La Commissione adotta atti di esecuzione che stabiliscono norme dettagliate relative alla determinazione dei diritti che l'ENISA deve riscuotere, specificando in particolare i costi stimati imputabili a ciascuna delle prestazioni per le quali possono essere riscossi diritti a norma dei paragrafi 1, 2 e 3 e l'ammontare dei singoli diritti esigibili, nonché le modalità e le condizioni di pagamento dei diritti. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2. Nel preparare tali progetti di atti di esecuzione, la Commissione consulta l'ENISA.
6. I diritti determinati mediante gli atti di esecuzione di cui al paragrafo 5 sono stabiliti in anticipo in modo da risultare proporzionati ai costi stimati delle attività svolte o dei servizi prestati, determinati in modo efficace sotto il profilo dei costi, e sono sufficienti a coprire detti costi. Tutte le spese dell'ENISA attribuite al personale impegnato nelle attività di cui ai paragrafi 1, 2 e 3 concorrono alla formazione dei costi da coprire. I diritti sono fissati a un livello tale da evitare un disavanzo o un significativo accumulo di eccedenze nel bilancio dell'ENISA. Le eccedenze di bilancio generate dalla riscossione dei diritti sono riportate per finanziare le attività dell'ENISA, in particolare le attività future correlate a diritti, o per compensare le perdite subite. Nel caso si registri regolarmente un saldo positivo significativo del bilancio, risultante dalle attività coperte dai diritti, o in caso di saldo negativo significativo risultante dalla prestazione dei servizi coperti dai diritti, la Commissione modifica gli atti di esecuzione di cui al paragrafo 5 per rivedere il metodo di calcolo dei diritti in conformità dell'articolo 118, paragrafo 2.

L'importo dei diritti per quanto riguarda i compiti di cui al paragrafo 1 è fissato a un livello che assicuri entrate sufficienti a contribuire alla copertura dei costi delle attività connesse allo sviluppo e al mantenimento dei sistemi europei di attestazione individuale, al trattamento delle domande e al rilascio e al rinnovo delle autorizzazioni, nonché dei costi necessari per tali attività di sorveglianza da parte dell'ENISA.

L'importo dei diritti per quanto riguarda i compiti di cui al paragrafo 2 è fissato a un livello che assicuri entrate sufficienti a contribuire alla copertura integrale dei costi delle attività connesse al mantenimento dei sistemi europei di certificazione della cibersicurezza di cui all'articolo 75.

L'importo dei diritti per quanto riguarda i compiti di cui al paragrafo 3 è fissato a un livello che assicuri entrate sufficienti a contribuire alla copertura dei costi delle attività connesse alla fornitura degli strumenti di prova di cui all'articolo 15, paragrafo 1.
7. L'ENISA presenta una relazione sui diritti riscossi e sulla loro incidenza sul suo bilancio nell'ambito della procedura di rendicontazione di cui all'articolo 50.
8. L'ENISA predispone una serie di indicatori per misurare il carico di lavoro, l'efficacia e l'efficienza in relazione alle attività finanziate mediante diritti. L'ENISA adegua di conseguenza la pianificazione del personale e la gestione delle risorse relative ai diritti in modo tale da poter rispondere in maniera adeguata a tali richieste e a eventuali variazioni delle entrate derivanti da diritti. L'ENISA condivide la

relazione con la Commissione, che può utilizzarla ai fini della valutazione di cui all'articolo 120, paragrafo 1.

Articolo 48
Esecuzione del bilancio dell'ENISA

1. Il direttore esecutivo è responsabile dell'esecuzione del bilancio dell'ENISA ed esercita le funzioni di ordinatore.
2. Il revisore contabile interno della Commissione esercita nei confronti dell'ENISA le stesse competenze di cui dispone nei confronti dei servizi della Commissione.
3. Il direttore esecutivo trasmette ogni anno all'autorità di bilancio tutte le informazioni pertinenti ai risultati delle procedure di valutazione.

Articolo 49
Rendicontazione e discarico

1. Il contabile dell'ENISA comunica i conti provvisori per l'esercizio (anno N) al contabile della Commissione e alla Corte dei conti entro il 1° marzo dell'esercizio successivo (anno N + 1).
2. Il contabile dell'ENISA comunica inoltre al contabile della Commissione le informazioni contabili necessarie ai fini del consolidamento, secondo le modalità e il formato stabiliti da quest'ultimo, entro il 1° marzo dell'anno N + 1.
3. L'ENISA trasmette al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti una relazione sulla gestione finanziaria e di bilancio dell'anno N entro il 31 marzo dell'anno N + 1.
4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti provvisori dell'ENISA per l'anno N, il contabile dell'ENISA redige i conti definitivi dell'ENISA sotto la propria responsabilità. Il direttore esecutivo li presenta al consiglio di amministrazione per parere.
5. Il consiglio di amministrazione formula un parere sui conti definitivi dell'ENISA per l'anno N.
6. Entro il 1° luglio dell'anno N + 1 il contabile dell'ENISA trasmette i conti definitivi dell'ENISA per l'anno N, accompagnati dal parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.
7. Un link alle pagine del sito web contenente i conti definitivi dell'ENISA è pubblicato nella *Gazzetta ufficiale dell'Unione europea* entro il 15 novembre dell'anno N + 1.
8. Entro il 30 settembre dell'anno N + 1 il direttore esecutivo invia alla Corte dei conti una risposta alle osservazioni formulate da quest'ultima nella sua relazione annuale. Il direttore esecutivo trasmette tale risposta anche al consiglio di amministrazione e alla Commissione.
9. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo, tutte le informazioni necessarie al corretto svolgimento della procedura di discarico per l'anno N, in conformità dell'articolo 267, paragrafo 3, del regolamento (UE, Euratom) 2024/2509 del Parlamento europeo e del Consiglio.

10. Il Parlamento europeo, su raccomandazione del Consiglio che delibera a maggioranza qualificata, concede il discarico al direttore esecutivo, entro il 15 maggio dell'anno N + 2, per l'esecuzione del bilancio dell'anno N.

Articolo 50

Regolamentazione finanziaria

1. La regolamentazione finanziaria applicabile all'ENISA è adottata dal consiglio di amministrazione previa consultazione della Commissione. Essa si discosta dal regolamento delegato (UE) 2019/715 solo per esigenze specifiche di funzionamento dell'ENISA e previo accordo della Commissione.
2. L'ENISA stabilisce ed esegue il proprio bilancio conformemente alla regolamentazione finanziaria ad essa applicabile e al regolamento (UE, Euratom) 2024/2509.

Articolo 51

Lotta antifrode

1. Ai fini della lotta contro la frode, la corruzione e altre attività illecite, alle attività dell'ENISA si applicano senza limitazioni le disposizioni del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio⁷⁵.
2. L'ENISA aderisce all'accordo interistituzionale, del 25 maggio 1999, tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo alle indagini interne svolte dall'Ufficio europeo per la lotta antifrode (OLAF)⁷⁶ entro sei mesi a decorrere dal [OP: inserire la data esatta di cui all'articolo 127] e adotta le opportune disposizioni applicabili al suo personale utilizzando il modello riportato nell'allegato di tale accordo.
3. La Corte dei conti ha potere di verifica, esercitabile su documenti e mediante controlli in loco, su tutti i beneficiari di sovvenzioni, i contraenti e i subappaltatori che hanno beneficiato di fondi dell'Unione da parte dell'ENISA.
4. L'OLAF può svolgere indagini, compresi controlli e verifiche sul posto, al fine di accertare l'esistenza di frodi, corruzione o ogni altra attività illecita lesiva degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dall'ENISA, conformemente alle disposizioni e alle procedure previste dal regolamento (UE, Euratom) n. 883/2013 e dal regolamento (Euratom, CE) n. 2185/96⁷⁷ del Consiglio.
5. Fatti salvi i paragrafi da 1 a 4, gli accordi di lavoro con paesi terzi e organizzazioni internazionali, i contratti, le convenzioni di sovvenzione e le decisioni di sovvenzione dell'ENISA contengono disposizioni che autorizzano esplicitamente la

⁷⁵ Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1, ELI: <http://data.europa.eu/eli/reg/2013/883/oj>).

⁷⁶ GU L 136 del 31.5.1999, pag. 15, ELI: http://data.europa.eu/eli/agree_interinst/1999/531/oj.

⁷⁷ Regolamento (Euratom, CE) n. 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2, ELI: <http://data.europa.eu/eli/reg/1996/2185/oj>).

Corte dei conti e l'OLAF a procedere a tali revisioni contabili e indagini conformemente alle loro rispettive competenze.

6. A norma del regolamento (UE) 2017/1939 del Consiglio l'EPPO può svolgere indagini ed esercitare l'azione penale in relazione a frodi e altre attività illegali che ledono gli interessi finanziari dell'Unione secondo quanto disposto dalla direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio⁷⁸.

Articolo 52

Dichiarazione di interessi

1. I membri del consiglio di amministrazione, il direttore esecutivo, il vicedirettore esecutivo, come pure i funzionari distaccati dagli Stati membri a titolo temporaneo, rendono ciascuno una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza. Le dichiarazioni sono precise e complete, presentate ogni anno per iscritto e aggiornate ogniqualvolta sia necessario.
2. I membri del consiglio di amministrazione, il direttore esecutivo, il vicedirettore esecutivo e gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano ciascuno in modo preciso e completo, al più tardi all'inizio di ogni riunione, qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del giorno e si astengono dal partecipare alle discussioni e alle votazioni inerenti tali punti.
3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per le regole sulle dichiarazioni di interessi di cui ai paragrafi 1 e 2.

Articolo 53

Trasparenza

1. L'ENISA svolge le proprie attività con un livello elevato di trasparenza e nel rispetto dell'articolo 55.
2. L'ENISA provvede a che al pubblico e alle parti interessate siano fornite informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubblicamente disponibili le dichiarazioni di interessi rese conformemente all'articolo 52.
3. Il consiglio di amministrazione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività dell'ENISA.
4. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2.

⁷⁸

Direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio, del 5 luglio 2017, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (GU L 198 del 28.7.2017, pag. 29, ELI: <http://data.europa.eu/eli/dir/2017/1371/oj>).

Articolo 54
Riservatezza all'interno dell'ENISA

1. Fatto salvo l'articolo 55, l'ENISA non divulga a terzi le informazioni da essa trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato.
2. I membri del consiglio di amministrazione, il direttore esecutivo, il vicedirettore esecutivo, i membri del gruppo consultivo ENISA, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'ENISA, compresi i funzionari distaccati dagli Stati membri a titolo temporaneo, rispettano gli obblighi di riservatezza di cui all'articolo 339 TFUE anche dopo la cessazione delle proprie funzioni.
3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di riservatezza di cui ai paragrafi 1 e 2.

Articolo 55
Accesso ai documenti

1. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dall'ENISA.
2. Il consiglio di amministrazione adotta disposizioni per l'attuazione del regolamento di esecuzione (CE) n. 1049/2001.
3. Le decisioni adottate dall'ENISA a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono formare oggetto di una denuncia presentata al Mediatore europeo a norma dell'articolo 228 TFUE o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 TFUE.

Capo V
Personale e funzionari di collegamento

Articolo 56
Disposizioni generali

1. Al personale dell'ENISA si applicano lo statuto dei funzionari, il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per dare applicazione allo statuto dei funzionari e al regime applicabile agli altri agenti.
2. Il personale dell'ENISA, i funzionari di collegamento e gli esperti nazionali distaccati presso l'ENISA sono sottoposti a un'adeguata procedura per il rilascio del nulla osta di sicurezza.

Articolo 57
Privilegi e immunità

All'ENISA e al suo personale si applica il protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea, allegato al TFUE.

Articolo 58
Funzionari di collegamento

1. Ciascuno Stato membro designa almeno due funzionari di collegamento di un'autorità nazionale competente designata a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555 quali esperti nazionali distaccati presso l'ENISA affinché prestino servizio nella sede o nell'ufficio locale di quest'ultima, in conformità dell'articolo 59, paragrafo 2. Anche la Commissione può designare un funzionario di collegamento.
2. I funzionari di collegamento contribuiscono all'esecuzione dei compiti dell'ENISA, anche agevolando la cooperazione operativa e lo scambio di informazioni di cui all'articolo 11. Sostengono inoltre l'ENISA nella diffusione di informazioni sulle attività, sui risultati e sulle raccomandazioni che la riguardano presso i pertinenti portatori di interessi in tutta l'Unione. Fungono altresì da punti di contatto nazionali per le domande poste dai rispettivi Stati membri e concernenti questi ultimi, rispondendo direttamente a tali domande o ponendosi in contatto con le amministrazioni nazionali interessate.
3. I funzionari di collegamento designati dai rispettivi Stati membri hanno la facoltà di richiedere e ricevere da questi ultimi tutte le informazioni pertinenti, come previsto dal presente regolamento, nel pieno rispetto del diritto nazionale e delle prassi vigenti negli Stati membri, in particolare per quanto riguarda la protezione dei dati e la riservatezza.

Articolo 59
Esperti nazionali distaccati e altro personale

1. L'ENISA può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze, in qualsiasi ambito delle sue attività. Lo statuto dei funzionari e il regime applicabile agli altri agenti non si applicano a tale personale.
2. Il consiglio di amministrazione adotta una decisione che stabilisce le regole relative al distacco di esperti nazionali, compresi i funzionari di collegamento, presso l'ENISA.

Capo VI
DISPOSIZIONI GENERALI RELATIVE ALL'ENISA

Articolo 60
Status giuridico dell'ENISA

1. L'ENISA è un organismo dell'Unione con personalità giuridica.
2. L'ENISA gode, in ciascuno Stato membro, della più ampia capacità giuridica riconosciuta alle persone giuridiche dal diritto nazionale di tale Stato membro. In particolare, può acquistare o alienare beni mobili e immobili e stare in giudizio.
3. L'ENISA è rappresentata dal direttore esecutivo.

Articolo 61
Sede

L'ENISA ha sede ad Atene, Grecia.

Articolo 62
Accordo sulla sede e condizioni operative

1. Le necessarie disposizioni relative all'insediamento dell'ENISA nello Stato membro ospitante e alle strutture che quest'ultimo deve mettere a disposizione nonché le regole specifiche applicabili in tale Stato membro al direttore esecutivo, ai membri del consiglio di amministrazione, al personale dell'ENISA e ai membri delle rispettive famiglie sono fissate in un accordo di sede concluso tra l'ENISA e lo Stato membro ospitante, previa approvazione del consiglio di amministrazione.
2. Lo Stato membro che ospita l'ENISA fornisce le migliori condizioni possibili volte a garantire il corretto funzionamento dell'ENISA, tenendo conto dell'accessibilità della sede, dell'esistenza di strutture scolastiche adeguate per i figli del personale, di un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi dei membri del personale.

Articolo 63
Controllo amministrativo

Il Mediatore europeo vigila sull'operato dell'ENISA conformemente all'articolo 228 TFUE.

Articolo 64
Responsabilità dell'ENISA

1. La responsabilità contrattuale dell'ENISA è disciplinata dal diritto applicabile al contratto.
2. La Corte di giustizia dell'Unione europea è competente a giudicare in virtù di clausole compromissorie contenute nel contratto concluso dall'ENISA.
3. In materia di responsabilità extracontrattuale, l'ENISA è obbligata al risarcimento dei danni cagionati da essa o dai membri del suo personale nell'esercizio delle loro funzioni, secondo i principi generali comuni agli ordinamenti degli Stati membri.
4. La Corte di giustizia dell'Unione europea è competente a conoscere delle controversie relative al risarcimento dei danni di cui al paragrafo 3.
5. La responsabilità personale del personale dell'ENISA nei confronti dell'ENISA è disciplinata dalle disposizioni ad esso applicabili dello statuto dei funzionari e del regime applicabile agli altri agenti.

Articolo 65
Regime linguistico

1. All'ENISA si applica il regolamento n. 1 del Consiglio⁷⁹. Gli Stati membri e gli altri organismi designati dagli Stati membri possono rivolgersi all'ENISA e ottenere la risposta in una delle lingue ufficiali delle istituzioni dell'Unione di loro scelta.
2. I servizi di traduzione e tutti gli altri servizi linguistici necessari per il funzionamento dell'ENISA, ad eccezione dell'interpretazione, sono forniti dal Centro di traduzione degli organismi dell'Unione europea.

⁷⁹ Regolamento del Consiglio n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU L7 del 6.10.1958, pag. 385, ELI: [http://data.europa.eu/eli/reg/1958/1\(1\)/oj](http://data.europa.eu/eli/reg/1958/1(1)/oj)).

Articolo 66
Protezione dei dati personali

1. Il trattamento dei dati personali da parte dell'ENISA è soggetto al regolamento (UE) 2018/1725.
2. Il consiglio di amministrazione adotta le norme di attuazione di cui all'articolo 45, paragrafo 3, del regolamento (UE) 2018/1725. Il consiglio di amministrazione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (UE) 2018/1725 da parte dell'ENISA.

Articolo 67
Regole in materia di sicurezza per la protezione delle informazioni sensibili non classificate e delle informazioni classificate

D'intesa con la Commissione, l'ENISA adotta regole in materia di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni sensibili non classificate e delle ICUE di cui alle decisioni (UE, Euratom) 2015/443⁸⁰ e (UE, Euratom) 2015/444⁸¹. Tali regole in materia di sicurezza disciplinano, tra l'altro, lo scambio, il trattamento e la conservazione di tali informazioni.

Articolo 68
Cooperazione con i soggetti dell'Unione e le autorità nazionali

1. Per garantire coerenza, creare sinergie e affrontare questioni di interesse comune, l'ENISA coopera su questioni relative alla cibersicurezza con il CERT-UE e i pertinenti soggetti dell'Unione, tra cui Europol, il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca istituito a norma del regolamento (UE) 2021/887 e il comitato europeo per la protezione dei dati istituito a norma dell'articolo 68, paragrafo 1, del regolamento (UE) 2016/679.
2. La cooperazione di cui al paragrafo 1 può essere assicurata in particolare tramite:
 - a) lo scambio di know-how e migliori pratiche;
 - b) la fornitura di consulenza e l'emanazione di orientamenti su questioni relative alla cibersicurezza;
 - c) la definizione di disposizioni pratiche per l'esecuzione di compiti specifici, previa consultazione della Commissione.
3. L'ENISA intraprende una cooperazione strutturata con il CERT-UE, in particolare su questioni relative allo sviluppo delle capacità, alla cooperazione operativa e alle analisi strategiche a lungo termine delle minacce informatiche.
4. L'ENISA coopera e scambia informazioni con le autorità di vigilanza del mercato e le autorità di controllo competenti designate ai sensi della normativa dell'Unione in materia di cibersicurezza, compreso il regolamento (UE) 2024/2847.

⁸⁰ Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41, ELI: <http://data.europa.eu/eli/dec/2015/443/oj>).

⁸¹ Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53, ELI: <http://data.europa.eu/eli/dec/2015/444/oj>).

Articolo 69

Cooperazione con i portatori di interessi

1. Ove necessario per conseguire gli obiettivi del presente regolamento, l'ENISA coopera con i pertinenti portatori di interessi, quali il settore della cibersecurity, il settore delle TIC, le PMI, i soggetti che operano nei settori elencati negli allegati I e II della direttiva (UE) 2022/2555, i fabbricanti, gli importatori o i distributori di prodotti con elementi digitali ai sensi del regolamento (UE) 2024/2847, gli organismi di valutazione della conformità notificati nell'ambito del quadro europeo di certificazione della cibersecurity e del regolamento (UE) 2024/2847, i soggetti che operano nel settore dei mezzi di identificazione elettronica, le organizzazioni dei consumatori e gli esperti del mondo accademico nel settore della cibersecurity. A tal fine l'ENISA può istituire partenariati pubblico-privato.
2. L'ENISA, in consultazione con la Commissione, sostiene la cooperazione tra gli organismi di valutazione della conformità notificati a norma dell'articolo 93. In particolare può istituire un gruppo di organismi di valutazione della conformità notificati per la condivisione delle migliori pratiche, creando sinergie con altre normative pertinenti dell'Unione, in particolare il regolamento (UE) 2024/2847.

Articolo 70

Cooperazione con paesi terzi e organizzazioni internazionali

1. Nella misura necessaria ai fini del conseguimento degli obiettivi del presente regolamento, l'ENISA può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi, in linea con le priorità dell'Unione. A tal fine l'ENISA può istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali, previa approvazione da parte della Commissione. Detti accordi di lavoro non creano obblighi giuridici per l'Unione e gli Stati membri.
2. Il consiglio di amministrazione adotta una strategia per le relazioni con paesi terzi e organizzazioni internazionali riguardo a questioni che rientrano tra le competenze dell'ENISA e in linea con le priorità di cui al paragrafo 1. La Commissione garantisce che l'ENISA operi nell'ambito del proprio mandato e del quadro istituzionale vigente stipulando accordi di lavoro adeguati con il direttore esecutivo.
3. Per sostenere la cooperazione con i paesi terzi, in particolare i paesi candidati all'adesione all'Unione, l'ENISA può fornire le proprie competenze in materia di sviluppo delle capacità, in particolare nei seguenti settori:
 - a) valutazione del livello di maturità delle capacità e delle risorse di cibersecurity;
 - b) crescita e rafforzamento della forza lavoro nel settore della cibersecurity, anche promuovendo l'ECSF e i sistemi europei di attestazione delle competenze individuali in materia di cibersecurity e offrendo attività di apprendimento e formazione;
 - c) sostegno alla pianificazione e all'esecuzione di esercitazioni di cibersecurity.
4. L'ENISA è aperta alla partecipazione ai suoi lavori di paesi terzi che abbiano concluso con l'Unione accordi in tal senso. Nell'ambito delle pertinenti disposizioni degli accordi conclusi tra l'Unione e i paesi terzi, sono istituiti, previa approvazione della Commissione, accordi di lavoro che specificano, in particolare, la natura, la portata e le modalità di partecipazione di detti paesi terzi ai lavori dell'ENISA, e

comprendono disposizioni sulla partecipazione alle iniziative intraprese dall'ENISA, sui contributi finanziari e sul personale. In materia di personale, tali accordi di lavoro rispettano in ogni caso lo statuto dei funzionari e il regime applicabile agli altri agenti.

5. L'ENISA riferisce periodicamente al Consiglio e alla Commissione in merito all'attuazione degli accordi di lavoro di cui ai paragrafi 1 e 4.

Titolo III

QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Capo I

Obiettivi, ambito di applicazione e procedure

Articolo 71

Obiettivi e ambito di applicazione del quadro europeo di certificazione della cibersecurity

1. È istituito il quadro europeo di certificazione della cibersecurity al fine di creare un mercato unico digitale per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e i soggetti. A tal fine il quadro aumenta il livello di cibersecurity all'interno dell'Unione e rende possibile un approccio armonizzato ai sistemi europei di certificazione della cibersecurity, facendo inoltre leva sulla certificazione per agevolare il rispetto della normativa applicabile dell'Unione.
2. Il quadro europeo di certificazione della cibersecurity prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersecurity e ad attestare:
 - a) che i prodotti TIC, i servizi TIC e i processi TIC valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi, o accessibili tramite essi, per tutto il loro ciclo di vita;
 - b) che i servizi di sicurezza gestiti valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza ai fini della protezione della disponibilità, dell'autenticità, dell'integrità e della riservatezza dei dati consultati, trattati, conservati o trasmessi in relazione alla prestazione di tali servizi, e che tali servizi sono forniti continuamente con la competenza, la perizia e l'esperienza richieste da personale avente un livello sufficiente e adeguato di conoscenze tecniche pertinenti e integrità professionale;
 - c) che la postura di cibersecurity di un soggetto che è stato valutato nell'ambito di tali sistemi è conforme a determinati requisiti di cibersecurity.
3. La certificazione europea della cibersecurity è volontaria, salvo diversamente specificato nel diritto dell'Unione o nazionale.
4. Il certificato europeo di cibersecurity e la dichiarazione UE di conformità rilasciati nell'ambito del quadro europeo di certificazione della cibersecurity sono automaticamente riconosciuti in tutti gli Stati membri.

Articolo 72
Informazione e consultazione del pubblico

1. Almeno una volta all'anno la Commissione organizza, con il sostegno dell'ENISA, un'assemblea europea sulla certificazione della cibersecurity, invitando i membri dell'ECCG e altri esperti pertinenti degli Stati membri, gli esperti in materia dei soggetti dell'Unione e i pertinenti portatori di interessi a discutere delle priorità strategiche per l'armonizzazione nel settore della certificazione della cibersecurity.
2. La Commissione gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni sui seguenti aspetti:
 - a) sistemi europei di certificazione della cibersecurity di cui è stato richiesto lo sviluppo a norma dell'articolo 73;
 - b) priorità strategiche per l'armonizzazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti, della postura di cibersecurity dei soggetti o dei requisiti di sicurezza della normativa dell'Unione, compresi i potenziali settori per i quali potrebbe essere richiesto un sistema europeo di certificazione della cibersecurity.
3. La Commissione rende pubbliche sul sito web di cui al paragrafo 2 del presente articolo le informazioni concernenti la sua richiesta all'ENISA relativa alla preparazione di una proposta di sistema di cui all'articolo 73 e la sua decisione di accogliere, respingere o abbandonare la proposta di sistema trasmessa dall'ENISA in conformità dell'articolo 74, paragrafo 7.
4. Nel corso della preparazione di una proposta di sistema da parte dell'ENISA a norma dell'articolo 74, il Parlamento europeo e il Consiglio possono chiedere alla Commissione, in qualità di presidente dell'ECCG, e all'ENISA di presentare informazioni pertinenti sul progetto di proposta di sistema. Su richiesta del Parlamento europeo o del Consiglio, l'ENISA, d'intesa con la Commissione e fatto salvo l'articolo 54, può mettere a disposizione del Parlamento europeo e del Consiglio le parti pertinenti di un progetto di proposta di sistema con modalità adeguate al livello di riservatezza richiesto e, se del caso, limitate.
5. Il Parlamento europeo e il Consiglio possono invitare la Commissione e l'ENISA a discutere questioni relative all'attuazione dei sistemi europei di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti.

Articolo 73
Richieste relative alla preparazione di un sistema europeo di certificazione della cibersecurity

1. La Commissione può chiedere all'ENISA di preparare una proposta di sistema europeo di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti.
2. In casi debitamente giustificati, l'ECCG può suggerire alla Commissione di presentare una richiesta di cui al paragrafo 1.
3. La richiesta di cui al paragrafo 1 precisa la finalità, la portata e le modalità del conseguimento dei pertinenti obiettivi ed elementi di sicurezza di cui agli articoli 80 e 81. La richiesta precisa inoltre il piano di elaborazione della proposta di sistema

europeo di certificazione della cibersicurezza e le specifiche tecniche pertinenti di cui inserire un riferimento o da definire nel sistema.

4. Nel preparare la richiesta di cui al paragrafo 1, la Commissione consulta debitamente l'ENISA e l'ECCG e tiene conto delle opinioni di tutti i pertinenti portatori di interessi e di altri soggetti dell'Unione compresi, se del caso, quelli pertinenti ai sensi della normativa dell'Unione in base alla quale un sistema europeo di certificazione della cibersicurezza dimostra la conformità e conferisce una presunzione di conformità.

Articolo 74

Preparazione e adozione dei sistemi europei di certificazione della cibersicurezza

1. Entro 12 mesi dal ricevimento di una richiesta della Commissione a norma dell'articolo 73, salvo diversamente specificato nella richiesta, l'ENISA prepara una proposta di sistema europeo di certificazione della cibersicurezza che soddisfa i requisiti di cui agli articoli 80 e 81.
2. Per la preparazione di ciascuna proposta di sistema, l'ENISA istituisce un gruppo di lavoro ad hoc in conformità dell'articolo 32, paragrafo 6, il cui scopo è fornire all'ENISA una consulenza specialistica.
3. In sede di preparazione della proposta di sistema, l'ENISA coopera strettamente con l'ECCG. L'ECCG fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e, ove applicabile, delle relative specifiche tecniche.
4. In sede di preparazione della proposta di sistema e, ove applicabile, delle relative specifiche tecniche, l'ENISA consulta tempestivamente i portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo. L'ENISA coopera inoltre con le autorità pubbliche competenti degli Stati membri e con i pertinenti soggetti dell'Unione per raccogliere le loro consulenze specialistiche in relazione alla preparazione della proposta di sistema e, se del caso, delle relative specifiche tecniche. Quando trasmette la proposta di sistema alla Commissione a norma del paragrafo 6, l'ENISA descrive le modalità con cui si è conformata a tale paragrafo.
5. Prima di trasmettere alla Commissione la proposta di sistema e, se del caso, le relative specifiche tecniche, l'ENISA chiede ai membri dell'ECCG di fornire pareri scritti sulla proposta di sistema. I pareri sono forniti entro 30 giorni dalla data della richiesta. L'ENISA tiene nella massima considerazione i pareri dei membri dell'ECCG. L'assenza di tali pareri non impedisce all'ENISA di trasmettere la proposta di sistema alla Commissione.
6. L'ENISA trasmette la proposta di sistema alla Commissione entro 60 giorni dalla data della richiesta di cui al paragrafo 5.
7. Quando riceve la proposta di sistema, la Commissione valuta se il sistema corrisponda alla richiesta presentata a norma dell'articolo 73. Entro 30 giorni dalla data di trasmissione della proposta di sistema in questione, la Commissione intraprende una delle seguenti azioni:
 - a) accoglie la proposta di sistema;

- b) rinvia la proposta di sistema all'ENISA per revisione, fornendo le motivazioni di tale rinvio e fissando un termine non superiore a 90 giorni entro il quale l'ENISA fornisce una proposta di sistema riveduta;
 - c) abbandona la proposta di sistema.
8. Se la Commissione rinvia una proposta di sistema all'ENISA per revisione conformemente al paragrafo 7, lettera b), si applicano di conseguenza i paragrafi 4, 5 e 7.
9. Sulla base della proposta di sistema preparata dall'ENISA e accolta, alla Commissione sono conferite le competenze ai fini dell'adozione di atti di esecuzione che prevedano un sistema europeo di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti che soddisfa i requisiti di cui agli articoli 80 e 81. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
10. La Commissione può fare riferimento alle specifiche tecniche elaborate dall'ENISA negli atti di esecuzione di cui al paragrafo 9 del presente articolo, conformemente agli articoli 18 e 77.
11. La Commissione può specificare le condizioni per il riconoscimento internazionale dei certificati europei di cibersecurity negli atti di esecuzione di cui al paragrafo 9 del presente articolo, conformemente all'articolo 87.

Articolo 75

Mantenimento di un sistema europeo di certificazione della cibersecurity

1. Ciascun sistema europeo di certificazione della cibersecurity definisce una strategia di mantenimento. La strategia di mantenimento delinea le aspettative per quanto riguarda le attività di mantenimento, in particolare quelle connesse alle norme o alle specifiche tecniche cui è fatto riferimento nel sistema e all'interazione con i pertinenti portatori di interessi.
2. L'ENISA, in cooperazione con la Commissione e grazie al sostegno dell'ECCG e del suo pertinente sottogruppo per il mantenimento, garantisce il mantenimento dei sistemi europei di certificazione della cibersecurity, anche in considerazione di un'eventuale revisione di tali sistemi da parte della Commissione. L'ENISA coopera e scambia informazioni con i soggetti e i gruppi pertinenti dell'Unione in relazione alle attività di mantenimento.
3. L'ENISA può organizzare la partecipazione del settore privato al mantenimento di un sistema sotto forma di gruppo di lavoro ad hoc conformemente alla strategia di mantenimento di cui al paragrafo 1.
4. Le attività di mantenimento dei sistemi europei di certificazione della cibersecurity comprendono:
- a) la preparazione, l'aggiornamento e l'approvazione di specifiche tecniche e orientamenti a sostegno del funzionamento armonizzato e uniforme dei sistemi;
 - b) l'individuazione di norme o specifiche tecniche pertinenti per il sistema;
 - c) interazioni e, se del caso, la creazione di collegamenti con i pertinenti portatori di interessi, comprese le organizzazioni di normazione europee o internazionali, anche al fine di fornire o ricevere contributi tecnici;

- d) la formulazione di raccomandazioni rivolte alla Commissione per quanto riguarda i necessari miglioramenti e aggiornamenti dei sistemi, anche in considerazione di un'eventuale revisione degli stessi;
 - e) lo scambio di informazioni relative all'attuazione pratica dei sistemi tra gli Stati membri;
 - f) contributi ai meccanismi di revisione e valutazione tra pari e all'analisi dei risultati di tali valutazioni per migliorare il funzionamento dei sistemi e agevolarne l'eventuale revisione.
5. L'ECCG può formulare un parere sul mantenimento dei sistemi europei di certificazione della ciphersicurezza.

Articolo 76

Valutazione, revisione e ritiro di un sistema europeo di certificazione della ciphersicurezza

1. Almeno ogni quattro anni dopo l'entrata in applicazione di un sistema europeo di certificazione della ciphersicurezza l'ENISA valuta l'impatto e l'efficacia di tale sistema, in cooperazione con il pertinente sottogruppo dell'ECCG per il mantenimento e tenendo conto dei riscontri ricevuti dai portatori di interessi. L'ENISA effettua la valutazione attraverso un'analisi di mercato conformemente all'articolo 8, paragrafo 1.
2. A seguito della valutazione di cui al paragrafo 1, la Commissione può rivedere o ritirare gli atti di esecuzione che prevedono un sistema europeo di certificazione della ciphersicurezza a norma dell'articolo 74, paragrafo 9.
3. In sede di revisione o di ritiro di sistemi europei di certificazione della ciphersicurezza, la Commissione consulta l'ENISA, l'ECCG e il relativo sottogruppo sul mantenimento e tiene altresì conto delle opinioni dei pertinenti portatori di interessi e di altri soggetti dell'Unione.
4. L'ECCG può formulare un parere sulla revisione o sul ritiro di un sistema europeo di certificazione della ciphersicurezza. La Commissione ne tiene debitamente conto in sede di revisione o di ritiro del sistema europeo di certificazione della ciphersicurezza.

Articolo 77

Specifiche tecniche nei sistemi europei di certificazione della ciphersicurezza

1. L'ENISA può elaborare specifiche tecniche in vista di un futuro sistema europeo di certificazione della ciphersicurezza o a sostegno del mantenimento di un sistema europeo di certificazione della ciphersicurezza.
2. Le specifiche tecniche di cui al paragrafo 1 del presente articolo sono elaborate tempestivamente, con il sostegno dell'ECCG e dei suoi sottogruppi per il mantenimento e, ove applicabile, del corrispondente gruppo di lavoro ad hoc di cui all'articolo 75, paragrafo 3. A tal fine l'ENISA chiede inoltre ai pertinenti gruppi di portatori di interessi di fornire il loro contributo, tenendo conto della strategia di mantenimento di cui all'articolo 75, paragrafo 1.
3. Qualora siano richiamate in un sistema europeo di certificazione della ciphersicurezza come previsto all'articolo 74, paragrafo 10, le specifiche tecniche sono rese disponibili sul sito web di cui all'articolo 79.

4. In casi debitamente giustificati, in particolare se contengono informazioni che potrebbero compromettere la sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti certificati o della postura di cibersicurezza dei soggetti certificata, le specifiche tecniche sono distribuite solo ai soggetti interessati dai requisiti del sistema. Le specifiche tecniche non sono richiamate in un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 74, paragrafo 10.

Articolo 78

Agevolazione della conformità alla legislazione dell'Unione

1. Se un atto giuridico specifico dell'Unione lo prevede, un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza dimostra la conformità e conferisce una presunzione di conformità alle corrispondenti prescrizioni di tale atto giuridico.
2. Le attività di valutazione nell'ambito di un sistema europeo di certificazione della cibersicurezza sono coerenti con il corrispondente atto giuridico dell'Unione che prevede la dimostrazione di conformità e la presunzione di conformità. Se tali attività di valutazione non sono specificate nel corrispondente atto giuridico dell'Unione, il sistema le specifica. La valutazione della conformità per la certificazione che conferisce la presunzione di conformità alle prescrizioni della normativa dell'Unione è effettuata da un organismo terzo.
3. In assenza di una normativa armonizzata dell'Unione, anche il diritto nazionale può disporre che un sistema europeo di certificazione della cibersicurezza possa essere utilizzato per dimostrare la conformità e stabilire la presunzione di conformità alle prescrizioni giuridiche specifiche stabilite nel diritto nazionale.

Articolo 79

Diffusione dei sistemi europei di certificazione della cibersicurezza, sito web dell'ENISA e pubblicazione dei certificati

1. L'ENISA organizza attività volte a promuovere la diffusione dei sistemi europei di certificazione della cibersicurezza adottati, anche gestendo il sito web di cui al paragrafo 2 del presente articolo.
2. L'ENISA gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni pubbliche riguardanti:
 - a) i sistemi europei di certificazione della cibersicurezza;
 - b) i diritti associati al mantenimento di ciascun sistema europeo di certificazione della cibersicurezza;
 - c) le pertinenti specifiche tecniche dell'ENISA;
 - d) i certificati europei di cibersicurezza e le dichiarazioni UE di conformità, comprese le informazioni sui certificati e sulle dichiarazioni che non sono più validi o che sono sospesi, revocati o scaduti;
 - e) le pertinenti informazioni supplementari sulla cibersicurezza fornite in conformità dell'articolo 84;
 - f) le sintesi delle revisioni tra pari a norma dell'articolo 89, paragrafo 7;
 - g) le specifiche tecniche richiamate in un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 74, paragrafo 10.

3. Ove applicabile, il sito web di cui al paragrafo 2 indica inoltre i sistemi di certificazione della cibersecurity nazionali che sono stati sostituiti da un sistema europeo di certificazione della cibersecurity.

Capo II

Contenuto dei sistemi europei di certificazione della cibersecurity

Articolo 80

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersecurity

1. Un sistema europeo di certificazione della cibersecurity persegue, a seconda del caso, gli obiettivi di sicurezza seguenti:
- a) garantire che i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita;
 - b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla conservazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati utilizzando mezzi tecnici adeguati e tenendo conto dell'intero ciclo di vita dei prodotti TIC, dei servizi TIC o dei processi TIC;
 - c) proteggere l'integrità dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e delle configurazioni da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore e segnalare le corruzioni, tenendo conto dell'intero ciclo di vita dei prodotti TIC, dei servizi TIC o dei processi TIC;
 - d) garantire la protezione dall'accesso non autorizzato mediante meccanismi di controllo adeguati, tra cui, a titolo esemplificativo ma non esaustivo, sistemi di autenticazione e di gestione dell'identità o dell'accesso, e segnalare eventuali accessi non autorizzati;
 - e) individuare e documentare i componenti e le vulnerabilità, provvedendo anche, ove opportuno, a redigere una distinta dei materiali del software che includa almeno le dipendenze di primo livello;
 - f) fornire informazioni sulla sicurezza registrando e monitorando le attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi, ove applicabile, con un meccanismo di disattivazione per l'utilizzatore;
 - g) verificare che i prodotti TIC, i servizi TIC e i processi TIC non contengano vulnerabilità sfruttabili note;
 - h) proteggere la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di attenuazione contro gli attacchi di negazione del servizio (*denial of service*);
 - i) ridurre al minimo l'impatto negativo sulla disponibilità dei servizi forniti da altri dispositivi e da altre reti in caso di incidente fisico o tecnico;
 - j) garantire che i prodotti TIC, i servizi TIC e i processi TIC siano periodicamente sottoposti a prove e a una valutazione della loro sicurezza;
 - k) garantire che le vulnerabilità siano affrontate e corrette senza indugio, anche mediante aggiornamenti di sicurezza, e che siano condivise e divulgate

pubblicamente informazioni sulle vulnerabilità risolte, salvo qualora i rischi legati alla divulgazione siano superiori ai benefici in termini di sicurezza;

- l) garantire che sia messa in atto una politica di divulgazione coordinata delle vulnerabilità;
- m) facilitare la condivisione di informazioni sulle potenziali vulnerabilità dei prodotti TIC, dei servizi TIC e dei processi TIC;
- n) garantire che siano diffusi tempestivamente aggiornamenti di sicurezza, qualora disponibili, per risolvere i problemi di sicurezza individuati;
- o) garantire che i servizi di sicurezza gestiti siano forniti con la competenza, la perizia e l'esperienza richieste e il personale responsabile della prestazione di tali servizi possieda un livello sufficiente e adeguato di conoscenze e competenze tecniche nel settore specifico, un'esperienza sufficiente e appropriata e la massima integrità professionale;
- p) garantire che i prodotti TIC, i servizi TIC e i processi TIC avviati nella fornitura dei servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita e, se del caso, includano gli ultimi aggiornamenti connessi alla sicurezza e non contengano vulnerabilità note;
- q) garantire che il soggetto certificato predisponga procedure interne appropriate affinché i servizi forniti abbiano un livello di qualità sufficiente e adeguato;
- r) garantire che il soggetto certificato sia in grado di individuare gli incidenti, rilevarli, proteggersi da essi, rispondervi e riprendersi dai medesimi;
- s) provvedere affinché il soggetto certificato sia in grado di gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che il soggetto utilizza nelle sue attività o nella fornitura dei suoi servizi, nonché prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei suoi servizi e per altri servizi;
- t) provvedere affinché il soggetto certificato sia in grado di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa provvedendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, a predisporre l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informativi e di rete che sono utilizzati dal soggetto e su cui si fondano la continuità della fornitura dei servizi e la loro qualità, anche in occasione di perturbazioni;
- u) garantire che il soggetto certificato sia in grado di attuare e mantenere un sistema di gestione della sicurezza delle informazioni;
- v) resistere a qualsiasi evento che possa compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti dal sistema informativo e di rete utilizzato dal soggetto o accessibili attraverso tale sistema, e garantire la continuità della fornitura dei servizi e la loro qualità, anche in occasione di perturbazioni;
- w) provvedere affinché il soggetto sia in grado di garantire la sicurezza del trattamento dei dati personali.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 119 per modificare il paragrafo 1 del presente articolo aggiungendo o modificando obiettivi di sicurezza, al fine di garantire che essi riflettano i più recenti sviluppi tecnologici e le nuove minacce correlate, nonché di adottare nuovi atti

legislativi dell'Unione che stabiliscano che la certificazione europea della cibersecurity può essere utilizzata per dimostrare la conformità e la presunzione di conformità ai pertinenti requisiti di cibersecurity previsti da tali atti legislativi.

3. Un sistema europeo di certificazione della cibersecurity per i prodotti con elementi digitali quali definiti all'articolo 3, punto 1), del regolamento (UE) 2024/2847 è progettato in conformità dei requisiti essenziali di cibersecurity di cui all'allegato I di detto regolamento e tiene conto delle norme armonizzate disponibili.

Articolo 81

Elementi dei sistemi europei di certificazione della cibersecurity

1. Un sistema europeo di certificazione della cibersecurity comprende almeno i seguenti elementi:
 - a) l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo o le categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, oppure le risorse, i servizi e le funzioni del soggetto che rientrano nell'ambito di applicazione della certificazione;
 - b) una descrizione chiara dello scopo del sistema e, se del caso, l'individuazione della legislazione dell'Unione che stabilisce i requisiti in relazione ai quali i certificati europei di cibersecurity dimostrano la conformità e conferiscono una presunzione di conformità;
 - c) la strategia di mantenimento che specifica l'approccio alle attività di mantenimento di cui all'articolo 75;
 - d) gli specifici requisiti di cibersecurity, criteri e metodi di valutazione da utilizzare per la valutazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity dei soggetti, nonché i riferimenti alle norme internazionali, europee o nazionali applicate nella valutazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity dei soggetti o, laddove tali norme non siano disponibili o adeguate, alle specifiche tecniche elaborate dall'ENISA a norma dell'articolo 77 oppure, se tali specifiche non sono disponibili, ad altre specifiche tecniche;
 - e) il periodo massimo di validità dei certificati europei di cibersecurity rilasciati nell'ambito del sistema.
2. Un sistema europeo di certificazione della cibersecurity comprende almeno regole e condizioni riguardanti:
 - a) il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity dei soggetti ai requisiti dei certificati europei di cibersecurity o delle dichiarazioni UE di conformità, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersecurity specificati;
 - b) il rilascio, la conferma, la revoca e il rinnovo dei certificati europei di cibersecurity, l'ampliamento o la riduzione dell'ambito di applicazione della certificazione e la nuova certificazione;
 - c) le conseguenze per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o i soggetti che sono stati certificati o per i quali è stata

rilasciata una dichiarazione UE di conformità, ma che non sono conformi ai requisiti del sistema;

- d) il modo in cui segnalare e trattare le vulnerabilità della cibersecurity nei prodotti TIC, servizi TIC e processi TIC precedentemente non rilevate;
- e) il contenuto e il formato dei certificati europei di cibersecurity e le dichiarazioni UE di conformità da rilasciare;
- f) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti che devono essere rese disponibili dal fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o dal soggetto la cui postura di cibersecurity è oggetto di certificazione;
- g) eventuali meccanismi di valutazione tra pari istituiti nell'ambito del sistema per le autorità o gli organismi che rilasciano certificati europei di cibersecurity a norma dell'articolo 85, paragrafo 4, i quali non pregiudicano la revisione tra pari di cui all'articolo 90;
- h) la riservatezza delle informazioni e dei dati ottenuti da tutte le parti nello svolgimento dei compiti e delle attività connessi all'attuazione delle disposizioni di cui al presente titolo;
- i) il formato e le procedure che i fabbricanti o i fornitori di prodotti TIC, servizi TIC o processi TIC devono rispettare nel fornire e aggiornare le informazioni supplementari sulla cibersecurity a norma dell'articolo 84; e
- j) la continuità delle attività di certificazione in situazioni di crisi straordinarie che sono inevitabili e ostacolano la possibilità di applicare le regole del sistema di certificazione.

3. Un sistema europeo di certificazione della cibersecurity comprende, se del caso, anche quanto segue:

- a) uno o più livelli di affidabilità e i corrispondenti livelli di valutazione;
- b) i profili di protezione per specificare i requisiti di sicurezza applicabili a una determinata categoria di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti;
- c) i profili di estensione per definire requisiti di sicurezza supplementari, compresi, ove applicabile, i requisiti di sicurezza stabiliti nelle disposizioni nazionali di recepimento del diritto dell'Unione;
- d) i chiarimenti in merito a quali attività di valutazione della conformità, tra cui tarature, prove, certificazioni e ispezioni, per il livello di affidabilità "elevato" o per dimostrare la conformità e conferire la presunzione di conformità, siano consentite al di fuori dello Spazio economico europeo (SEE);
- e) l'individuazione dei sistemi nazionali o internazionali di certificazione della cibersecurity relativi allo stesso tipo o alle stesse categorie di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o postura di cibersecurity dei soggetti;
- f) i requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cibersecurity;

- g) le informazioni che sono necessarie per la certificazione e che un richiedente deve fornire agli organismi di valutazione della conformità o mettere altrimenti a loro disposizione;
 - h) i marchi o le etichette e le condizioni alle quali tali marchi o etichette possono essere utilizzati;
 - i) le condizioni per il riconoscimento internazionale dei certificati europei di cibersecurity conformemente all'articolo 87.
- 4. I requisiti specificati del sistema europeo di certificazione della cibersecurity sono coerenti con le prescrizioni della legislazione dell'Unione.
 - 5. Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscano principi comuni e disposizioni tipo per gli elementi di cui ai paragrafi 1, 2 e 3 in tutti i sistemi europei di certificazione della cibersecurity. Un sistema europeo di certificazione della cibersecurity può includere riferimenti a tali principi e disposizioni tipo, se del caso e ove disponibili.
 - 6. Gli atti di esecuzione di cui al paragrafo 5 sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2. Nell'elaborare o rivedere i principi comuni e le disposizioni tipo per gli elementi dei sistemi europei di certificazione della cibersecurity, la Commissione consulta l'ENISA e tiene conto, ove opportuno, delle opinioni dell'ECCG, dei pertinenti portatori di interessi e di altri organismi pertinenti.

Articolo 82

Livelli di affidabilità e valutazione dei sistemi europei di certificazione della cibersecurity

- 1. I sistemi europei di certificazione della cibersecurity possono specificare per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti uno o più dei livelli di affidabilità seguenti: "di base", "sostanziale" o "elevato". Tali livelli di affidabilità sono commisurati al livello di rischio associato al previsto uso del prodotto TIC, del servizio TIC, processo TIC o servizio di sicurezza gestito, o alla natura dei soggetti la cui postura di cibersecurity è oggetto di certificazione e al loro ambiente operativo, in termini di probabilità e impatto di un incidente.
- 2. I certificati europei di cibersecurity si riferiscono a qualsiasi livello di affidabilità specificato nel sistema europeo di certificazione della cibersecurity nell'ambito del quale si rilasciano tali certificati. Le dichiarazioni UE di conformità si riferiscono al livello di affidabilità "di base".
- 3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersecurity pertinente, compresi i corrispondenti controlli di sicurezza e la relativa valutazione a cui è necessario sottoporre il prodotto TIC, il servizio TIC, il processo TIC, il servizio di sicurezza gestito o la postura di cibersecurity del soggetto.
- 4. Il certificato europeo di cibersecurity o la dichiarazione UE di conformità si riferiscono a specifiche tecniche, norme e procedure ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cibersecurity, o prevenirli.
- 5. Un certificato europeo di cibersecurity o una dichiarazione UE di conformità che si riferisca al livello di affidabilità "di base" assicura che i prodotti TIC, i servizi TIC, i

processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti per i quali è rilasciato tale certificato o è rilasciata tale dichiarazione UE di conformità soddisfano i corrispondenti requisiti di sicurezza, compresi i controlli di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

6. Un certificato europeo di cibersecurity che si riferisca al livello di affidabilità "sostanziale" assicura che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti per i quali è rilasciato soddisfano i corrispondenti requisiti di sicurezza, compresi i controlli di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti di incidenti e di attacchi informatici e il rischio di attacchi informatici da parte di soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o i soggetti attuano correttamente i necessari controlli di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.
7. Un certificato europeo di cibersecurity che si riferisca al livello di affidabilità "elevato" assicura che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti per i quali è rilasciato soddisfano i corrispondenti requisiti di sicurezza, compresi i controlli di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di incidenti e di attacchi informatici avanzati commessi da soggetti che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno:
 - a) un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note;
 - b) un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o i soggetti attuano correttamente i necessari controlli di sicurezza, allo stato tecnologico più avanzato;
 - c) una valutazione della resistenza dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o dei soggetti agli attacchi commessi da soggetti qualificati, ricorrendo, se del caso, a test di penetrazione.

Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente. Tutte le attività di valutazione della conformità, comprese tarature, prove, certificazioni e ispezioni, per il livello di affidabilità "elevato" sono intraprese nello Spazio economico europeo, salvo diversamente previsto in un sistema europeo di certificazione della cibersecurity.

8. Qualora un sistema europeo di certificazione della cibersecurity sia concepito per dimostrare la conformità e conferire la presunzione di conformità a uno specifico atto giuridico dell'Unione, un certificato europeo di cibersecurity assicura che i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti che sono stati certificati soddisfano i corrispondenti requisiti di cibersecurity previsti da tale atto giuridico. Tutte le attività di valutazione della conformità, comprese tarature, prove, certificazioni e ispezioni, ai fini della presunzione di conformità sono intraprese nello Spazio economico europeo,

salvo diversamente previsto in un sistema europeo di certificazione della cibersecurity.

9. Un sistema europeo di certificazione della cibersecurity può precisare vari livelli di valutazione per un determinato livello di affidabilità. Ciascun livello di valutazione corrisponde a uno dei livelli di affidabilità.

Articolo 83

Autovalutazione della conformità

1. Un sistema europeo di certificazione della cibersecurity può consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o del soggetto la cui postura di cibersecurity è oggetto di certificazione. L'autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, ai servizi TIC, ai processi TIC, ai servizi di sicurezza gestiti o alla postura di cibersecurity dei soggetti che presentano un basso rischio corrispondente al livello di affidabilità "di base".
2. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o il soggetto la cui postura di cibersecurity è oggetto di certificazione può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema europeo di certificazione della cibersecurity. Rilasciando tale dichiarazione, tale fabbricante, fornitore o soggetto si assume la responsabilità della conformità del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito o della postura di cibersecurity ai requisiti previsti in tale sistema.
3. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o il soggetto la cui postura di cibersecurity è oggetto di certificazione rende disponibile all'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 89, per il periodo stabilito nel sistema europeo di certificazione della cibersecurity, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità al sistema dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity. Una copia della dichiarazione UE di conformità è trasmessa senza indebito ritardo all'autorità nazionale di certificazione della cibersecurity e all'ENISA.

Articolo 84

Informazioni supplementari sulla cibersecurity dei prodotti TIC, servizi TIC e processi TIC certificati

1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC per i quali è stata rilasciata una dichiarazione UE di conformità o un certificato europeo di cibersecurity mettono a disposizione dell'utente le seguenti informazioni supplementari sulla cibersecurity:
 - a) la finalità prevista del prodotto TIC, servizio TIC o processo TIC in questione, compreso l'ambiente di sicurezza fornito dal fabbricante o fornitore;
 - b) orientamenti e raccomandazioni che assistano gli utenti nel configurare, installare, avviare, operare e mantenere in modo sicuro i prodotti TIC o servizi TIC;

- c) il tipo di assistenza tecnica di sicurezza offerta dal fabbricante o fornitore e la data finale del periodo di assistenza durante il quale gli utilizzatori possono aspettarsi che le vulnerabilità siano gestite e di ricevere gli aggiornamenti di sicurezza;
 - d) se il fabbricante o fornitore decide di mettere a disposizione dell'utilizzatore la distinta dei materiali del software, informazioni sul luogo in cui è possibile accedere a tale distinta.
2. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC per i quali è stata rilasciata una dichiarazione UE di conformità o è stato rilasciato un certificato europeo di cibersecurity rende pubblicamente disponibili le seguenti informazioni supplementari sulla cibersecurity:
- a) il punto di contatto unico dove è possibile segnalare e ricevere informazioni sulle vulnerabilità e dove è possibile reperire la politica del fabbricante sulla divulgazione coordinata delle vulnerabilità;
 - b) informazioni sulle vulnerabilità risolte, compresa una descrizione delle vulnerabilità, tra cui informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritengano che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, i fabbricanti o fornitori possono ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità di applicare la pertinente patch.
3. Le informazioni di cui ai paragrafi 1 e 2 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, durante il periodo di validità e per almeno cinque anni dopo la scadenza o la revoca del certificato europeo di cibersecurity o della dichiarazione UE di conformità pertinente.
4. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano qualora la sicurezza del prodotto TIC, servizio TIC o processo TIC pertinente possa essere compromessa dalla divulgazione pubblica delle informazioni.

Capo III

Governance del quadro europeo di certificazione della cibersecurity

Sezione 1

Disposizioni generali e gestione dei sistemi europei di certificazione della cibersecurity

Articolo 85

Rilascio di certificati europei di cibersecurity

1. I prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti che sono stati certificati nell'ambito di un sistema europeo di certificazione della cibersecurity sono considerati conformi ai requisiti di tale sistema.

2. Gli organismi di valutazione della conformità di cui all'articolo 91 rilasciano certificati europei di cibersecurity sulla base dei criteri previsti dal sistema europeo di certificazione della cibersecurity adottato a norma dell'articolo 74.
3. In deroga al paragrafo 2, un sistema europeo di certificazione della cibersecurity può prevedere che i certificati europei di cibersecurity derivanti da tale sistema possano essere rilasciati unicamente da uno degli organismi pubblici seguenti:
 - a) un'autorità nazionale di certificazione della cibersecurity di cui all'articolo 88 accreditata come organismo di valutazione della conformità a norma dell'articolo 91, paragrafo 1;
 - b) un organismo pubblico accreditato come organismo di valutazione della conformità a norma dell'articolo 91, paragrafo 1.
4. Ove un sistema europeo di certificazione della cibersecurity adottato a norma dell'articolo 74 preveda un livello di affidabilità "elevato" o laddove specificato diversamente da tale sistema, il certificato europeo di cibersecurity nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cibersecurity di cui all'articolo 88 accreditata come organismo di valutazione della conformità a norma dell'articolo 91, paragrafo 1, oppure nei casi seguenti:
 - a) da un organismo di valutazione della conformità sulla base di un modello di previa approvazione; o
 - b) da un organismo di valutazione della conformità sulla base di un modello di delega generale.
5. Alla Commissione è conferito il potere di adottare atti di esecuzione che specifichino le procedure per il modello di previa approvazione o di delega generale di cui al paragrafo 4 del presente articolo. Nell'elaborare tali atti di esecuzione la Commissione consulta l'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
6. La persona fisica o giuridica che presenta i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per la certificazione o il soggetto che richiede la certificazione della propria postura di cibersecurity mette a disposizione dell'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 89, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersecurity, o dell'organismo di valutazione della conformità di cui all'articolo 91 tutte le informazioni necessarie a espletare la certificazione.
7. Gli organismi di valutazione della conformità e, se del caso, le autorità nazionali di certificazione della cibersecurity informano l'ENISA senza indebito ritardo in merito alle loro decisioni che incidono sullo stato dei certificati europei di cibersecurity e delle dichiarazioni UE di conformità a norma dell'articolo 94.
8. Il titolare di un certificato europeo di cibersecurity informa l'organismo di valutazione della conformità e, se del caso, l'autorità nazionale di certificazione della cibersecurity di cui al paragrafo 7 delle eventuali vulnerabilità o non conformità successivamente rilevate, in relazione al prodotto TIC, al servizio TIC, al processo TIC o al servizio di sicurezza gestito certificato o alla postura di cibersecurity del soggetto, che hanno la probabilità di incidere sulla conformità al certificato. Tale organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersecurity interessata e valuta l'impatto sul certificato in linea con le condizioni del sistema indicate all'articolo 81, paragrafo 2, lettera d).

9. Per i loro prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti certificati che sono identificati, interamente o in parte, come risorse chiave a norma dell'articolo 102, i titolari di un certificato europeo di cibersicurezza non utilizzano, installano o integrano in altro modo componenti TIC o componenti che comprendono componenti TIC di fornitori ad alto rischio nei prodotti TIC, nei servizi TIC, nei processi TIC o nei servizi di sicurezza gestiti certificati.
10. Un certificato europeo di cibersicurezza è rilasciato per il periodo indicato nel sistema europeo di certificazione della cibersicurezza e può essere rinnovato, purché continuino a essere soddisfatti i requisiti pertinenti.
11. La Commissione coopera con gli Stati membri per garantire l'applicazione delle disposizioni relative al rilascio di certificati europei di cibersicurezza anche ai fini dell'applicazione dell'articolo 100, paragrafo 4, lettera b). L'organismo di valutazione della conformità e, se del caso, l'autorità nazionale di certificazione della cibersicurezza forniscono alla Commissione, su richiesta e senza indebito ritardo, tutte le informazioni relative al rilascio dei certificati europei di cibersicurezza o delle dichiarazioni UE di conformità pertinenti.

Articolo 86

Sistemi e certificati nazionali di certificazione della cibersicurezza

1. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersicurezza dei soggetti che rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 74, paragrafo 9. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersicurezza dei soggetti che non rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza possono restare in vigore.
2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza o procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersicurezza dei soggetti che già rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.
3. I certificati esistenti che sono stati rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza e che rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza restano validi fino alla loro data di scadenza.
4. Gli Stati membri informano la Commissione e l'ECCG prima di adottare nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersicurezza dei soggetti.
5. La Commissione può suggerire a uno Stato membro di ritirare un sistema nazionale di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersicurezza dei soggetti qualora lo sviluppo di un sistema europeo di certificazione della cibersicurezza che copre i prodotti, i servizi, i processi o la postura di cibersicurezza in questione sia già stato

richiesto a norma dell'articolo 73, tenendo conto del piano di sviluppo di detto sistema.

Articolo 87

Riconoscimento internazionale dei certificati europei di cibersecurity

1. I certificati di paesi terzi relativi a prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti e alla postura di cibersecurity dei soggetti possono essere riconosciuti, mediante un atto di esecuzione o attraverso la conclusione di un accordo tra l'Unione e il paese terzo in questione o un'organizzazione internazionale, come equivalenti ai certificati europei di cibersecurity se i requisiti del pertinente sistema del paese terzo o dell'organizzazione internazionale sono considerati equivalenti a quelli dei sistemi europei di certificazione della cibersecurity. Alla Commissione è conferito il potere di adottare tali atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
2. Gli atti di esecuzione e gli accordi di cui al paragrafo 1 si basano sulle condizioni per il riconoscimento internazionale dei certificati europei di cibersecurity stabilite conformemente all'articolo 74, paragrafo 11.
3. Gli accordi sul riconoscimento dei certificati di paesi terzi o dei certificati delle organizzazioni internazionali di cui al paragrafo 1 sono conclusi solo se riconoscono anche l'equivalenza dei certificati europei di cibersecurity ai certificati di paesi terzi.

Articolo 88

Autorità nazionali di certificazione della cibersecurity

1. Ciascuno Stato membro designa una o più autorità nazionali di certificazione della cibersecurity nel suo territorio oppure, con l'accordo di un altro Stato membro, una o più autorità nazionali di certificazione della cibersecurity in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.
2. Ciascuno Stato membro comunica alla Commissione l'identità delle autorità nazionali di certificazione della cibersecurity designate. Se uno Stato membro designa più di una autorità, comunica alla Commissione anche i compiti assegnati a ciascuna di tali autorità.
3. Ciascuna autorità nazionale di certificazione della cibersecurity è indipendente dai soggetti sui quali vigila per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale.
4. Le attività delle autorità nazionali di certificazione della cibersecurity relative al rilascio di certificati europei di cibersecurity a norma del presente regolamento sono rigorosamente separate dalle attività di vigilanza indicate nel presente articolo e all'articolo 85, paragrafo 4, lettere a) e b) e tali attività sono svolte indipendentemente le une dalle altre.
5. Gli Stati membri provvedono affinché le autorità nazionali di certificazione della cibersecurity dispongano di risorse adeguate per l'esercizio dei loro poteri e per l'esecuzione efficiente ed efficace dei loro compiti.
6. Le autorità nazionali di certificazione della cibersecurity svolgono i seguenti compiti:

- a) partecipano all'ECCG a norma dell'articolo 90, paragrafo 2;
- b) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersecurity a norma dell'articolo 81, paragrafo 2, lettera a), per garantire la conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e della postura di cibersecurity dei soggetti ai requisiti dei certificati europei di cibersecurity rilasciati nei rispettivi territori, in cooperazione con le autorità di vigilanza del mercato o le autorità di controllo competenti, comprese le autorità competenti a norma della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio⁸² o del regolamento (UE) 2024/2847;
- c) controllano, in cooperazione con le autorità di vigilanza del mercato competenti, la conformità agli obblighi che, ai sensi del presente regolamento, incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o ai soggetti la cui postura di cibersecurity è certificata che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità nel corrispondente sistema europeo di certificazione della cibersecurity, e fanno applicare tali obblighi;
- d) fatto salvo l'articolo 91, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento o altre autorità pertinenti nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento;
- e) cooperano con la Commissione qualora la competenza di un organismo di valutazione della conformità sia contestata a norma dell'articolo 94;
- f) vigilano sulle attività degli organismi pubblici di cui all'articolo 85, paragrafo 3, e le monitorano;
- g) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 93, controllano la conformità ai requisiti specifici o supplementari stabiliti nei sistemi europei di certificazione della cibersecurity a norma dell'articolo 81, paragrafo 3, lettera f), facendo applicare gli obblighi che incombono agli organismi di valutazione della conformità in relazione a tali requisiti, e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità non si conformino alle prescrizioni del presente regolamento;
- h) trattano i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersecurity rilasciati dalle autorità nazionali di certificazione della cibersecurity o ai certificati europei di cibersecurity rilasciati dagli organismi di valutazione della conformità ai sensi dell'articolo 85, paragrafo 4, oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 83, e svolgono le indagini opportune sull'oggetto di tali reclami e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole;

⁸² Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

- i) trasmettono alla Commissione, all'ENISA e all'ECCG una relazione annuale sulle loro principali attività entro il 31 marzo di ogni anno a decorrere dal [anno di entrata in vigore + 12 mesi] e la mettono a disposizione del gruppo incaricato della revisione tra pari ove l'autorità nazionale di certificazione della cibersecurity sia soggetta a una revisione tra pari a norma dell'articolo 89;
 - j) cooperano con le altre autorità nazionali di certificazione della cibersecurity, con le autorità di vigilanza del mercato o con altre autorità pubbliche, anche mediante lo scambio di informazioni sull'eventuale non conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e della postura di cibersecurity dei soggetti ai requisiti stabiliti dal presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersecurity;
 - k) monitorano gli sviluppi che presentano un interesse nel campo della certificazione della cibersecurity.
7. Ciascuna autorità nazionale di certificazione della cibersecurity dispone almeno dei seguenti poteri:
- a) richiedere agli organismi di valutazione della conformità, ai titolari di certificati europei della cibersecurity e agli emittenti di dichiarazioni UE di conformità di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;
 - b) condurre indagini, sotto forma di audit, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersecurity e degli emittenti di dichiarazioni UE di conformità allo scopo di verificare che rispettino le prescrizioni di cui al presente titolo;
 - c) adottare misure appropriate, nel rispetto del diritto nazionale, per accertare che gli organismi di valutazione della conformità, i titolari di certificati europei di cibersecurity e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersecurity;
 - d) ottenere accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersecurity al fine di svolgere indagini conformemente alla legislazione dell'Unione o al diritto processuale nazionale;
 - e) revocare, conformemente al diritto nazionale, i certificati europei di cibersecurity rilasciati dalle autorità nazionali di certificazione della cibersecurity o dagli organismi di valutazione della conformità in conformità dell'articolo 85, paragrafo 4, qualora tali certificati non siano conformi al presente regolamento o a un sistema europeo di certificazione della cibersecurity;
 - f) irrogare sanzioni conformemente al diritto nazionale, a norma dell'articolo 97, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.
8. Le autorità nazionali di certificazione della cibersecurity cooperano tra di loro e con la Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersecurity e le questioni tecniche riguardanti la cibersecurity dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti e la postura di cibersecurity dei soggetti.

9. Entro il [entrata in vigore + 6 mesi] l'ENISA elabora un modello per la relazione di cui al paragrafo 6, lettera i), del presente articolo, in cooperazione con la Commissione e l'ECCG.

Articolo 89
Revisione tra pari

1. Le autorità nazionali di certificazione della cibersecurity sono soggette a una revisione tra pari.
2. La revisione tra pari è effettuata sulla base di criteri e procedure di valutazione solidi e trasparenti, in particolare per quanto riguarda i requisiti in termini strutturali, di risorse umane e procedurali, la riservatezza e i reclami.
3. La revisione tra pari esamina:
 - a) ove applicabile, se le attività delle autorità nazionali di certificazione della cibersecurity relative al rilascio di certificati europei di cibersecurity di cui al presente regolamento siano rigorosamente separate dalle attività di vigilanza indicate all'articolo 88 e se tali attività siano svolte indipendentemente le une dalle altre;
 - b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e della postura di cibersecurity dei soggetti ai certificati europei di cibersecurity a norma dell'articolo 88, paragrafo 7, lettera a);
 - c) le procedure di monitoraggio e applicazione degli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o ai soggetti la cui postura di cibersecurity è certificata, a norma dell'articolo 88, paragrafo 7, lettera b);
 - d) le procedure di monitoraggio, autorizzazione e vigilanza delle attività degli organismi di valutazione della conformità.
4. La revisione tra pari è effettuata almeno una volta ogni cinque anni da almeno due autorità nazionali di certificazione della cibersecurity di altri Stati membri e dalla Commissione. L'ENISA può inoltre partecipare alla revisione tra pari in qualità di osservatore. Il gruppo incaricato della revisione tra pari redige la relazione finale e la sintesi della revisione tra pari.
5. L'ENISA sostiene l'organizzazione del meccanismo di revisione tra pari e delle revisioni tra pari, anche elaborando documenti di orientamento e modelli pertinenti, in cooperazione con la Commissione e l'ECCG.
6. Alla Commissione è conferito il potere di adottare atti di esecuzione che definiscano un piano almeno quinquennale per la revisione tra pari e fissino i criteri riguardanti la composizione del gruppo incaricato della revisione tra pari, la metodologia da utilizzare in tale revisione nonché il calendario, la frequenza e altri compiti ad essa connessi. Nell'elaborare tali atti di esecuzione la Commissione consulta l'ECCG e l'ENISA. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
7. La relazione finale, compresi eventuali orientamenti o raccomandazioni, e la sintesi della revisione tra pari sono esaminate dall'ECCG, che approva la sintesi per la pubblicazione sul sito web di cui all'articolo 79, paragrafo 2.

Articolo 90
Gruppo europeo per la certificazione della cibersecurity

1. È istituito il gruppo europeo per la certificazione della cibersecurity ("ECCG").
2. L'ECCG è composto da rappresentanti delle autorità nazionali di certificazione della cibersecurity o da rappresentanti di altre autorità nazionali competenti. Un membro dell'ECCG non rappresenta più di due Stati membri.
3. L'ECCG ha i seguenti compiti:
 - a) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti delle disposizioni del presente titolo, nelle questioni relative alla politica in materia di certificazione della cibersecurity e nel coordinamento degli approcci strategici;
 - b) consigliare e coadiuvare la Commissione nella preparazione delle richieste relative ai sistemi europei di certificazione della cibersecurity a norma dell'articolo 73;
 - c) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema ai sensi dell'articolo 74 e di specifiche tecniche ai sensi dell'articolo 77;
 - d) assistere, consigliare e collaborare con l'ENISA e la Commissione in relazione alle attività di mantenimento ai sensi dell'articolo 75;
 - e) assistere, consigliare e collaborare con la Commissione in relazione alla revisione o al ritiro di sistemi europei di certificazione della cibersecurity esistenti ai sensi dell'articolo 76;
 - f) proporre di trasmettere alla Commissione una richiesta relativa alla preparazione di una proposta di sistema europeo di certificazione della cibersecurity a norma dell'articolo 73, paragrafo 2;
 - g) adottare pareri indirizzati alla Commissione relativi al mantenimento, alla revisione e al ritiro degli attuali sistemi europei di certificazione della cibersecurity;
 - h) esaminare gli sviluppi pertinenti al settore della certificazione della cibersecurity, anche a livello nazionale ai sensi dell'articolo 86, e scambiare informazioni e buone pratiche sui sistemi europei di certificazione della cibersecurity;
 - i) agevolare la cooperazione tra le autorità nazionali di certificazione della cibersecurity secondo le prescrizioni del presente titolo attraverso lo sviluppo di capacità e lo scambio di informazioni, in particolare in relazione agli aspetti della certificazione della cibersecurity;
 - j) sostenere l'attuazione dei meccanismi di revisione tra pari a norma dell'articolo 89 e dei meccanismi di valutazione tra pari in conformità delle regole fissate in un sistema europeo di certificazione della cibersecurity ai sensi dell'articolo 81, paragrafo 2, lettera g);
 - k) agevolare l'allineamento dei sistemi europei di certificazione della cibersecurity alle norme riconosciute a livello internazionale, anche nell'ambito del mantenimento dei sistemi europei di certificazione della cibersecurity esistenti e, ove opportuno, rivolgere raccomandazioni all'ENISA

affinché collabori con le pertinenti organizzazioni di normazione europee o internazionali per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello europeo o internazionale.

4. Con l'assistenza dell'ENISA, la Commissione presiede l'ECCG e ne assicura il segretariato.
5. La Commissione può istituire sottogruppi dell'ECCG per una delle finalità seguenti:
 - a) esaminare questioni specifiche sulla base di un mandato stabilito dalla Commissione;
 - b) mantenere e rivedere i sistemi europei di certificazione in conformità del presente regolamento e sulla base di un mandato stabilito dalla Commissione.
6. I sottogruppi riferiscono all'ECCG.
7. I sottogruppi sono copresieduti dalla Commissione e dall'ENISA e quest'ultima ne assicura il segretariato.
8. L'ECCG e i suoi sottogruppi adottano il regolamento interno a maggioranza semplice dei loro membri, sulla base di una proposta della Commissione e d'intesa con quest'ultima.

Sezione 2

Organismi di valutazione della conformità

Articolo 91

Competenza degli organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008. Tale accreditamento è rilasciato solo se l'organismo di valutazione della conformità soddisfa i requisiti indicati nell'allegato I del presente regolamento.
2. Ove un certificato europeo di cibersecurity sia rilasciato da un'autorità nazionale di certificazione della cibersecurity a norma del presente regolamento, l'organismo di certificazione dell'autorità nazionale di certificazione della cibersecurity è accreditato come organismo di valutazione della conformità a norma del paragrafo 1.
3. L'accREDITamento di cui al paragrafo 1 è rilasciato agli organismi di valutazione della conformità per un periodo massimo di cinque anni e può essere rinnovato, purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Entro un termine ragionevole, gli organismi nazionali di accREDITamento adottano tutte le misure necessarie per limitare, sospendere o revocare l'accREDITamento di un organismo di valutazione della conformità rilasciato in virtù del paragrafo 1 se le condizioni per l'accREDITamento non sono state soddisfatte o non sono più soddisfatte oppure se l'organismo di valutazione della conformità non è conforme al presente regolamento.
4. Nello stabilire requisiti di accREDITamento specifici o supplementari per un sistema europeo di certificazione della cibersecurity relativo a prodotti TIC, a norma dell'articolo 92, si perseguono sinergie, ove opportuno, con i requisiti relativi agli organismi notificati a norma del regolamento (UE) 2024/2847 e con i requisiti di accREDITamento nell'ambito dei sistemi di certificazione della cibersecurity già adottati.

5. Qualora un organismo di valutazione della conformità sia accreditato a norma del regolamento (UE) 2024/2847, le autorità competenti possono riutilizzare come prove, durante il processo di accreditamento a norma del presente regolamento, i risultati di precedenti processi di accreditamento per quanto riguarda eventuali sovrapposizioni di requisiti.

Articolo 92

Ulteriore armonizzazione della competenza degli organismi di valutazione della conformità

1. Qualora un sistema europeo di certificazione della cibersecurity stabilisca requisiti specifici o supplementari a norma dell'articolo 81, paragrafo 3, lettera f), gli organismi di valutazione della conformità sono autorizzati da un'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 88, paragrafo 1, a svolgere i compiti previsti da tale sistema. Tale autorizzazione è rilasciata solo se l'organismo di valutazione della conformità è stato accreditato e soddisfa i requisiti specifici o supplementari stabiliti nell'ambito del sistema europeo di certificazione della cibersecurity.
2. Qualora richieda un'autorizzazione a norma del presente articolo, un organismo di valutazione della conformità trasmette la richiesta all'autorità nazionale di certificazione della cibersecurity dello Stato membro in cui è stabilito o all'autorità nazionale di certificazione della cibersecurity alla quale tale Stato membro ha fatto ricorso in conformità dell'articolo 88, paragrafo 1.
3. Un organismo di valutazione della conformità può chiedere l'autorizzazione a un'autorità nazionale di certificazione della cibersecurity diversa da quella indicata al paragrafo 2 in una delle situazioni seguenti:
 - a) se l'autorità nazionale di certificazione della cibersecurity di cui al paragrafo 1 non procede all'autorizzazione relativamente alle attività di valutazione della conformità per le quali è richiesta l'autorizzazione;
 - b) se l'autorità nazionale di certificazione della cibersecurity di cui al paragrafo 1 non è stata sottoposta a una revisione tra pari in conformità dell'articolo 89 relativamente alle attività di valutazione della conformità per le quali è richiesta l'autorizzazione.
4. Se riceve una richiesta a norma del paragrafo 3, un'autorità nazionale di certificazione della cibersecurity ne informa l'autorità nazionale di certificazione della cibersecurity dello Stato membro in cui è stabilito l'organismo di valutazione della conformità richiedente. In tali casi l'autorità nazionale di certificazione della cibersecurity di tale Stato membro può partecipare al processo di autorizzazione in qualità di osservatore.
5. Un'autorità nazionale di certificazione della cibersecurity può chiedere a un'altra autorità nazionale di certificazione della cibersecurity di svolgere parti dell'attività di valutazione. In tal caso il certificato di autorizzazione è rilasciato dall'autorità richiedente.
6. L'autorizzazione di cui al paragrafo 1 è valida per un periodo non superiore al periodo di validità dell'accREDITAMENTO e può essere rinnovata a condizione che l'organismo di valutazione della conformità soddisfi i requisiti di cui al paragrafo 1 e che sia stato rinnovato anche il relativo accREDITAMENTO.

7. Le autorità nazionali di certificazione della cibersecurity adottano entro un termine ragionevole tutte le misure necessarie per limitare, sospendere o revocare l'autorizzazione di un organismo di valutazione della conformità rilasciata in virtù del paragrafo 1 se le condizioni per l'autorizzazione non sono state soddisfatte o non sono più soddisfatte, oppure se l'organismo di valutazione della conformità non si conforma al presente regolamento.
8. Alla Commissione è conferito il potere di adottare atti di esecuzione per stabilire le procedure, anche in materia di cooperazione transfrontaliera, per l'autorizzazione degli organismi di valutazione della conformità. Nell'elaborare gli atti di esecuzione la Commissione consulta l'ENISA e l'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.

Articolo 93

Notifica degli organismi di valutazione della conformità

1. Per ciascun sistema europeo di certificazione della cibersecurity le autorità nazionali di certificazione della cibersecurity di uno Stato membro notificano alla Commissione e agli altri Stati membri gli organismi di valutazione della conformità che sono stati accreditati e, ove applicabile, autorizzati a norma dell'articolo 92.
2. Le autorità nazionali di certificazione della cibersecurity effettuano la notifica di cui al paragrafo 1 utilizzando lo strumento elettronico di notifica sviluppato e gestito dalla Commissione.
3. Alla Commissione è conferito il potere di adottare atti di esecuzione per stabilire le circostanze, i formati e le procedure per le notifiche di cui al paragrafo 1 del presente articolo, compresa la procedura di opposizione da parte di altri Stati membri durante il processo di notifica, l'identificazione univoca degli organismi di valutazione della conformità, nonché le circostanze per la limitazione, la sospensione o il ritiro della notifica. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.

Articolo 94

Contestazione della competenza degli organismi di valutazione della conformità

1. La Commissione indaga sui casi in cui abbia dubbi o venga a conoscenza di dubbi sulla competenza di un organismo di valutazione della conformità ad adempiere le prescrizioni e le responsabilità che a esso incombono, o sul continuo adempimento, da parte di tale organismo, di tali prescrizioni e responsabilità.
2. L'autorità nazionale di certificazione della cibersecurity fornisce alla Commissione, su richiesta, tutte le informazioni relative alla base della notifica o del mantenimento della competenza dell'organismo di valutazione della conformità interessato.
3. La Commissione garantisce la riservatezza di tutte le informazioni sensibili raccolte nel corso delle sue indagini.
4. Se accerta che un organismo di valutazione della conformità non soddisfa o non soddisfa più i requisiti per la sua notifica, la Commissione informa in merito l'autorità nazionale di certificazione della cibersecurity e chiede a quest'ultima di adottare le misure correttive necessarie, incluso all'occorrenza il ritiro della notifica.
5. Gli Stati membri provvedono affinché sia disponibile una procedura di ricorso avverso le decisioni degli organismi notificati.

Articolo 95

Obbligo di informazione e conservazione a carico degli organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità informano l'autorità nazionale di certificazione della cbersicurezza:
 - a) di qualsiasi rifiuto, limitazione, sospensione o revoca di un certificato;
 - b) di qualsiasi circostanza che influisce sull'ambito e sulle condizioni della notifica di cui all'articolo 93, paragrafo 1;
 - c) di qualsiasi richiesta di informazioni che abbiano ricevuto dalle autorità di vigilanza del mercato in relazione ad attività di valutazione della conformità;
 - d) su richiesta, di qualsiasi attività di valutazione della conformità eseguita nell'ambito della loro notifica e di qualsiasi altra attività svolta, incluse quelle transfrontaliere e di subappalto.
2. Gli organismi di valutazione della conformità forniscono inoltre all'ENISA le informazioni di cui al paragrafo 1, lettera a), al fine di agevolare lo svolgimento dei suoi compiti a norma dell'articolo 79.
3. Gli organismi di valutazione della conformità forniscono senza indebito ritardo agli altri organismi di valutazione della conformità a norma del presente regolamento, le cui attività di valutazione della conformità sono simili e hanno come oggetto gli stessi prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o soggetti la cui postura di cbersicurezza è certificata, informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, ai risultati positivi delle valutazioni della conformità.
4. Gli organismi di valutazione della conformità mantengono un sistema di registri in cui sono contenuti tutti i documenti e le prove presentati o ricevuti in relazione a ciascuna valutazione e certificazione da essi effettuata. I registri sono conservati in modo sicuro e accessibile per il periodo necessario ai fini della certificazione e per almeno cinque anni dopo la scadenza o la revoca di un certificato europeo di cbersicurezza pertinente.

Sezione 3

Altre disposizioni

Articolo 96

Diritto di presentare un reclamo e diritto a un ricorso giurisdizionale effettivo

1. Le persone fisiche e giuridiche hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di cbersicurezza o, se il reclamo riguarda un certificato europeo di cbersicurezza rilasciato da un organismo di valutazione della conformità che agisce conformemente all'articolo 85, paragrafo 4, all'autorità nazionale di certificazione della cbersicurezza competente.
2. L'autorità o l'organismo a cui è stato presentato il reclamo informa il reclamante dello stato del procedimento, della decisione adottata e del diritto a un ricorso giurisdizionale effettivo di cui ai paragrafi 3 e 4.

3. Fatti salvi eventuali ricorsi amministrativi o altri ricorsi extragiudiziali, le persone fisiche e giuridiche hanno diritto a un ricorso giurisdizionale effettivo per quanto riguarda:
 - a) le decisioni assunte dall'autorità o dall'organismo di cui al paragrafo 1, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cbersicurezza detenuto da tali persone fisiche e giuridiche;
 - b) il mancato intervento relativamente a un reclamo presentato all'autorità o all'organismo di cui al paragrafo 1.
4. I procedimenti a norma del presente articolo sono presentati dinanzi ai tribunali dello Stato membro in cui ha sede l'autorità o l'organismo contro cui è mosso il ricorso giurisdizionale.

Articolo 97 *Sanzioni*

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente titolo e di violazione dei sistemi europei di certificazione della cbersicurezza e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.

Titolo IV **SICUREZZA DELLE CATENE DI APPROVVIGIONAMENTO DELLE TIC**

Capo I *Quadro per catene di approvvigionamento delle TIC affidabili*

Articolo 98 *Ambito di applicazione del quadro*

1. Il quadro per catene di approvvigionamento delle TIC affidabili prevede un meccanismo di sicurezza a livello dell'Unione volto ad affrontare i rischi di natura non tecnica nei settori ad alta criticità e in altri settori critici di cui alla direttiva (UE) 2022/2555. Il meccanismo individua le risorse TIC chiave nelle catene di approvvigionamento critiche delle TIC e stabilisce misure di attenuazione adeguate e proporzionate ai soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555.
2. Gli obblighi di cui al presente titolo lasciano impregiudicati gli obblighi stabiliti all'articolo 13 del regolamento (UE) 2024/2847 e nelle disposizioni nazionali di recepimento dell'articolo 21 della direttiva (UE) 2022/2555.
3. Le disposizioni di cui al presente capo non impediscono agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cbersicurezza nelle catene di approvvigionamento delle TIC, a condizione che tali disposizioni siano coerenti con i loro obblighi stabiliti dal diritto dell'Unione.

Articolo 99
Valutazioni dei rischi per la sicurezza

1. La Commissione o un gruppo di almeno tre Stati membri può chiedere al gruppo di cooperazione istituito dall'articolo 14 della direttiva (UE) 2022/2555 ("gruppo di cooperazione NIS") di effettuare valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza conformemente all'articolo 22 di tale direttiva. Ove effettuata a seguito di tale richiesta, la valutazione dei rischi per la sicurezza comprende in particolare la proposta identificazione delle risorse TIC chiave della rispettiva catena di approvvigionamento delle TIC, nonché dei principali autori delle minacce, dei rischi e delle vulnerabilità che interessano tali risorse. Nell'ambito delle valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza sono elaborati scenari di rischio e sono proposte misure per attenuare i rischi individuati.
2. Le valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza sono completate entro sei mesi dalla richiesta di cui al paragrafo 1. Su richiesta della Commissione, il gruppo di cooperazione NIS può concordare un periodo più breve.
3. Se ha motivi sufficienti per ritenere che vi sia una minaccia informatica significativa per la sicurezza dell'Unione in relazione a una catena di approvvigionamento delle TIC e che sia necessario intervenire per preservare il corretto funzionamento del mercato interno, la Commissione provvede senza indugio a:
 - a) consultare gli Stati membri in merito alla necessità di adottare una o più delle misure di attenuazione di cui all'articolo 103; e
 - b) effettuare una valutazione dei rischi per la sicurezza, tenendo conto della consultazione degli Stati membri. La valutazione dei rischi per la sicurezza comprende la proposta identificazione delle risorse TIC chiave, nonché dei principali autori delle minacce, dei rischi e delle vulnerabilità che interessano tali risorse. Nell'ambito della valutazione dei rischi per la sicurezza sono elaborati scenari di rischio e sono proposte misure per attenuare i rischi individuati.

Articolo 100
Designazione dei paesi terzi che destano preoccupazioni per la cibersicurezza

1. Quando, a seguito della valutazione dei rischi di cui all'articolo 99 o sulla base di altre fonti, come una dichiarazione pubblica a nome dell'Unione o di uno Stato membro, risulta che un paese terzo presenta un rischio grave e strutturale di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione verifica il rischio posto da tale paese, tenendo conto degli elementi seguenti:
 - a) l'esistenza nel paese terzo di normative che impongono ai soggetti sottoposti alla sua giurisdizione di comunicare alle autorità di detto paese terzo informazioni sulle vulnerabilità di software o hardware prima che siano noti casi di sfruttamento di tali vulnerabilità;
 - b) le pratiche esistenti nel paese terzo, dimostrate da fonti indipendenti, che impongono ai soggetti sottoposti alla giurisdizione del paese terzo di comunicare alle autorità di detto paese terzo informazioni sulle vulnerabilità di software o hardware prima che siano noti casi di sfruttamento di tali vulnerabilità;

- c) l'assenza di mezzi di ricorso giurisdizionali efficaci e di meccanismi di controllo indipendente e democratico in grado di risolvere le preoccupazioni individuate in materia di sicurezza, anche per quanto riguarda le pratiche esistenti di cui alla lettera b);
 - d) le informazioni circostanziate su uno o più incidenti causati da autori di minacce controllati da tale paese e operanti al di fuori del suo territorio che conducono attività o campagne informatiche dolose, e l'incapacità o la mancata volontà del paese terzo di cooperare con la Commissione o gli Stati membri per affrontare il rischio derivante dalle attività degli autori delle minacce;
 - e) le informazioni pertinenti derivanti da valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza o da relazioni degli Stati membri o di organizzazioni internazionali.
2. Se conclude, a seguito della verifica di cui al paragrafo 1, che un paese terzo presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione può, mediante un atto di esecuzione, designare tale paese terzo come paese che desta preoccupazioni per la cibersicurezza delle catene di approvvigionamento delle TIC. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
3. La Commissione riesamina periodicamente gli atti di esecuzione adottati conformemente al paragrafo 2.
4. I fornitori ad alto rischio non hanno il diritto di:
- a) partecipare alle fasi di elaborazione, valutazione o consultazione né alle decisioni riguardanti le norme europee e i prodotti della normazione europea di cui all'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012 e le specifiche comuni di cui all'articolo 27 del regolamento (UE) 2024/2847 nel settore della cibersicurezza;
 - b) richiedere il rilascio o essere titolari di certificati europei di cibersicurezza a norma del titolo III;
 - c) diventare organismi di valutazione della conformità accreditati a norma del titolo III;
 - d) presentare domanda per diventare fornitori autorizzati di attestati europei delle competenze individuali in materia di cibersicurezza a norma del titolo II, sezione 4;
 - e) partecipare a procedure di appalto pubblico, organizzate conformemente alla normativa di recepimento delle direttive 2014/24/UE e 2014/25/UE in relazione alla fornitura di componenti TIC o componenti che comprendono componenti TIC da utilizzare nelle risorse TIC chiave individuate in conformità dell'articolo 102;
 - f) partecipare a qualsiasi attività nell'ambito dei programmi e degli strumenti di finanziamento dell'Unione attuati in regime di gestione diretta e indiretta conformemente all'articolo 136 del regolamento (UE, Euratom) 2024/2509 e alla normativa settoriale dell'Unione, né a qualsiasi attività di finanziamento dell'Unione attuata in regime di gestione concorrente in relazione alla fornitura di componenti TIC o componenti che comprendono componenti TIC da utilizzare nelle risorse TIC chiave individuate in conformità dell'articolo 102.

Le autorità incaricate delle procedure di cui alle lettere da a) a f) effettuano le valutazioni necessarie ai fini del presente paragrafo. A tal fine le autorità possono altresì avvalersi dell'elenco di cui all'articolo 104.

5. Se un fornitore ad alto rischio ha già ottenuto un certificato europeo di cibersecurity a norma del titolo III, l'autorità competente lo revoca senza indebito ritardo.

Articolo 101

Meccanismo generale per la sicurezza delle catene di approvvigionamento delle TIC

Se il gruppo di cooperazione NIS ha effettuato una valutazione coordinata a livello dell'Unione dei rischi per la sicurezza a norma dell'articolo 99, paragrafo 1, del presente regolamento, o dopo il completamento della procedura in caso di minaccia informatica significativa per una catena di approvvigionamento delle TIC a norma dell'articolo 99, paragrafo 3, la Commissione può adottare le misure di cui all'articolo 102 e all'articolo 103, paragrafi 1 e 2.

Articolo 102

Individuazione delle risorse TIC chiave

1. Quando dalla valutazione dei rischi effettuata a norma dell'articolo 99, paragrafo 1 o 3, emergono rischi di cibersecurity significativi in relazione a una catena di approvvigionamento delle TIC, la Commissione ha il potere di adottare atti di esecuzione per individuare le risorse TIC chiave utilizzate per la fabbricazione di prodotti o la fornitura di servizi da parte di soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2 del presente regolamento.
2. Nell'individuare le risorse TIC chiave di cui al paragrafo 1, la Commissione tiene conto degli elementi seguenti:
 - a) l'eventualità che tali risorse abbiano funzioni essenziali e sensibili per il funzionamento dei prodotti fabbricati o dei servizi forniti dal soggetto del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555;
 - b) l'eventualità che gli incidenti, compresi quelli causati da vulnerabilità sfruttate relative a tali risorse, possano causare gravi perturbazioni delle catene di approvvigionamento delle TIC in tutto il mercato interno o determinare un'esfiltrazione di dati;
 - c) l'eventualità che esista una dipendenza da un numero limitato di fornitori di tali risorse;
 - d) i risultati delle valutazioni dei rischi di cui all'articolo 99.

Articolo 103

Misure di attenuazione nella catena di approvvigionamento delle TIC

1. Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscano, ove necessario per garantire un livello elevato di cibersecurity, ciberresilienza e fiducia all'interno dell'Unione, che al tipo specifico di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555 è vietato utilizzare, installare o integrare in qualsiasi forma nelle risorse TIC chiave individuate in conformità dell'articolo 102 componenti TIC o componenti che comprendono componenti TIC di fornitori ad alto rischio individuati conformemente all'articolo 104. Tali atti di esecuzione prevedono

adeguati periodi di transizione, durante i quali la Commissione pubblica l'elenco dei fornitori ad alto rischio di cui all'articolo 104, nonché termini supplementari per l'eliminazione graduale dei pertinenti componenti TIC e componenti che comprendono componenti TIC. Tali atti di esecuzione possono anche specificare i componenti TIC o i componenti che comprendono componenti TIC.

2. Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscano, ove necessario per garantire un livello elevato di cibersecurity, cyberresilienza e fiducia all'interno dell'Unione, che al tipo specifico di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555 si applicano una o più delle seguenti misure di attenuazione in relazione alla rispettiva catena di approvvigionamento delle TIC e in particolare alle risorse TIC chiave individuate conformemente all'articolo 102, al fine di attenuare i rischi individuati nelle valutazioni dei rischi per la sicurezza effettuate a norma dell'articolo 99:
 - a) applicazione degli obblighi di trasparenza per quanto riguarda la trasmissione all'autorità competente di informazioni sui fornitori nella catena di approvvigionamento delle TIC per le risorse TIC chiave individuate a norma dell'articolo 102;
 - b) divieto relativo ai trasferimenti di dati verso paesi terzi e all'elaborazione di dati da remoto da un paese terzo;
 - c) misure tecniche da sottoporre a audit da parte di terzi, tra cui:
 - i) ricorso all'elaborazione su dispositivo (*on-device processing*);
 - ii) segmentazione specifica dei sistemi di rete;
 - iii) disabilitazione di qualsiasi accesso fisico o da remoto alle risorse TIC chiave;
 - iv) disabilitazione di elementi non essenziali;
 - v) monitoraggio operativo della rete;
 - vi) verifica di hardware e software.
 - d) restrizioni relative al controllo operativo, compresa l'esternalizzazione di funzioni organizzative a fornitori di servizi gestiti;
 - e) restrizioni relative ai rapporti contrattuali tra il soggetto e i suoi fornitori;
 - f) obbligo di affidare l'erogazione, la gestione, il mantenimento del servizio o la relativa assistenza a personale selezionato dalle pertinenti autorità nazionali competenti;
 - g) diversificazione dell'approvvigionamento di componenti TIC o di componenti inclusi nei componenti TIC.
3. Nell'introdurre le misure di cui al paragrafo 2, la Commissione può definire requisiti tecnici e metodologici per le misure.
4. Prima di adottare gli atti di esecuzione di cui ai paragrafi 1 e 2, la Commissione valuta i rischi e le dipendenze potenziali, in particolare:
 - a) ove applicabile, il livello di rischio associato all'utilizzo, all'installazione o all'integrazione, in qualsiasi forma, di componenti TIC o di componenti che comprendono componenti TIC di fornitori ad alto rischio in risorse TIC chiave;

- b) i potenziali impatti economici e sociali che l'obbligo può avere sui soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555;
 - c) la disponibilità di fornitori alternativi a quelli ad alto rischio;
 - d) la potenziale perturbazione delle attività economiche e sociali transfrontaliere causata da un incidente che interessa la catena di approvvigionamento delle TIC di un soggetto.
- 5. Gli atti di esecuzione di cui ai paragrafi 1 e 2 del presente articolo sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2, e sono rivisti almeno ogni 36 mesi.
 - 6. In circostanze eccezionali che giustificano un intervento volto a preservare il corretto funzionamento del mercato interno e se la Commissione ha motivi sufficienti per ritenere che l'utilizzo, l'installazione o l'integrazione di componenti TIC o di componenti che comprendono componenti TIC di un soggetto specifico stabilito in un paese terzo o controllato da un paese terzo, da soggetti di un paese terzo o da un cittadino di un paese terzo rappresenti un rischio di cibersecurity di natura non tecnica significativo per le attività economiche o sociali di almeno tre Stati membri, la Commissione consulta senza indugio gli Stati membri in merito alla necessità di adottare misure a livello dell'Unione.
 - 7. Alla Commissione è conferito il potere di adottare atti di esecuzione per stabilire che a un tipo specifico di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555 è vietato utilizzare, installare o integrare componenti TIC o componenti che comprendono componenti TIC di un soggetto di cui al paragrafo 6. A tal fine essa consulta i soggetti dei tipi di cui agli allegati I e II della direttiva (UE) 2022/2555 potenzialmente interessati dal divieto. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2. Ove opportuno, prevedono periodi adeguati per l'eliminazione graduale di tali componenti TIC o componenti che comprendono componenti TIC. Tali atti di esecuzione possono anche specificare i componenti TIC o i componenti che comprendono componenti TIC oggetto del divieto. Tale divieto riguarda anche i componenti TIC o i componenti che comprendono componenti TIC di tutti i soggetti controllati dal soggetto specifico di cui al paragrafo 6.
 - 8. Gli atti di esecuzione di cui ai paragrafi 1, 2 e 7 possono inoltre specificare che le misure di attenuazione sono applicabili solo ai tipi di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555 aventi determinate dimensioni.
 - 9. L'articolo 100, paragrafo 4, si applica al soggetto specifico stabilito in un paese terzo o controllato da un paese terzo, da un soggetto di un paese terzo o da un cittadino di un paese terzo di cui al paragrafo 7.
 - 10. Gli atti di esecuzione adottati conformemente ai paragrafi 1, 2 e 7 che sono applicabili al tipo di soggetti di cui all'allegato I, punto 10, della direttiva (UE) 2022/2555 si applicano mutatis mutandis alle istituzioni, agli organi e agli organismi europei.

Articolo 104
Individuazione dei fornitori ad alto rischio

1. La Commissione, mediante atti di esecuzione, stila elenchi di fornitori ad alto rischio pertinenti ai fini dei divieti stabiliti negli atti di esecuzione adottati a norma dell'articolo 103, paragrafi 1 e 7, o del divieto di cui all'articolo 111, paragrafo 1.
2. La Commissione realizza a tal fine una mappatura dei fornitori di componenti TIC e di componenti che comprendono componenti TIC pertinenti ai fini del divieto di cui al paragrafo 1.

La Commissione effettua su tale base una valutazione iniziale per individuare quali dei fornitori oggetto della mappatura siano potenzialmente stabiliti in un paese terzo designato a norma dell'articolo 100 o controllati da tale paese terzo, da un soggetto stabilito in tale paese terzo o da un cittadino di tale paese terzo. La Commissione realizza inoltre una prima mappatura dei fornitori potenzialmente controllati dal soggetto di cui all'articolo 103, paragrafo 6.
3. La Commissione valuta il luogo di stabilimento nonché l'assetto proprietario e di controllo dei fornitori inizialmente individuati a norma del paragrafo 2, secondo comma.
4. Ai fini della valutazione di cui al paragrafo 3, la Commissione ha la facoltà di richiedere ai fornitori le informazioni necessarie. Qualora il fornitore non fornisca le informazioni necessarie entro il termine stabilito, la Commissione può concludere che il fornitore è stabilito in un paese terzo designato a norma dell'articolo 100 o è controllato da tale paese terzo, da soggetti di tale paese terzo o da cittadini di tale paese terzo. Qualora stia effettuando una valutazione ai fini dell'articolo 103, paragrafo 7, e il fornitore non fornisca le informazioni necessarie entro il termine stabilito, la Commissione può concludere che il fornitore è controllato da un soggetto designato in conformità di detto articolo. Le autorità competenti di cui all'articolo 112 condividono a loro volta, su richiesta, le informazioni pertinenti con la Commissione.
5. La Commissione condivide con il fornitore interessato le conclusioni preliminari relative alla valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo. La Commissione concede al fornitore la possibilità di essere ascoltato in merito a tali conclusioni preliminari.
6. La Commissione può chiedere a un'autorità competente di effettuare la valutazione iniziale del luogo di stabilimento e dell'assetto proprietario e di controllo di un fornitore, ove giustificato alla luce delle caratteristiche dell'attività di tale fornitore. Un'autorità competente può offrirsi di effettuare tale valutazione iniziale. La Commissione verifica tali conclusioni iniziali al fine di decidere se il fornitore debba essere incluso nell'elenco dei fornitori ad alto rischio.
7. La Commissione aggiorna regolarmente l'elenco dei fornitori ad alto rischio al fine di eliminare o aggiungere fornitori ad alto rischio. I fornitori ad alto rischio inclusi nell'elenco possono chiedere alla Commissione di effettuare una nuova valutazione del loro luogo di stabilimento e del loro assetto proprietario e di controllo, dietro presentazione di elementi attestanti i cambiamenti intervenuti a tale riguardo.
8. Qualora un'autorità competente rilevi, anche sulla base delle informazioni fornite da un soggetto del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555, l'eventuale necessità di inserire un fornitore in un elenco di fornitori ad alto rischio, essa ne informa senza indebito ritardo la Commissione.

Articolo 105

Esenzione per i soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersicurezza o controllati da soggetti di tale paese terzo

1. Un soggetto stabilito in un paese terzo che desta preoccupazioni per la cibersicurezza designato conformemente all'articolo 100, oppure controllato da soggetti di tale paese terzo, può presentare alla Commissione una richiesta motivata di esenzione:
 - a) dal divieto, imposto ai soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555, di utilizzare, installare o integrare in qualsiasi forma i propri componenti TIC o componenti che comprendono i propri componenti TIC nelle risorse TIC chiave di tali soggetti, in deroga all'articolo 111 o agli atti di esecuzione adottati a norma dell'articolo 103, paragrafo 1;
 - b) dal divieto di partecipare a procedure di appalto pubblico, organizzate conformemente alla normativa di recepimento della direttiva 2014/24/UE e della direttiva 2014/25/UE in relazione alla fornitura di componenti TIC o componenti che comprendono componenti TIC da utilizzare nelle risorse TIC chiave individuate in conformità dell'articolo 102, in deroga all'articolo 100, paragrafo 4.
2. La richiesta di cui al paragrafo 1:
 - a) specifica l'interesse del soggetto stabilito in un paese terzo che desta preoccupazioni per la cibersicurezza designato a norma dell'articolo 100, oppure controllato da soggetti di tale paese terzo, a beneficiare dell'esenzione di cui al paragrafo 1 del presente articolo; e
 - b) dimostra con prove chiare che saranno messe in atto misure di attenuazione efficaci per affrontare i rischi di natura non tecnica e garantire l'assenza di qualsiasi interferenza indebita da parte del paese terzo designato a norma dell'articolo 100 in relazione alla fornitura di componenti TIC o componenti che comprendono componenti TIC per l'utilizzo, l'installazione o l'integrazione nelle risorse TIC chiave di un soggetto del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555.
3. Alla Commissione è conferito il potere di adottare atti di esecuzione per specificare ulteriormente le condizioni di cui al paragrafo 2, lettera b), e per stabilire norme dettagliate riguardo alle procedure di cui al presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.
4. La Commissione valuta la richiesta di cui al paragrafo 1 tramite un processo equo e trasparente, prendendo in considerazione:
 - a) le circostanze e gli elementi aggiuntivi di cui all'articolo 100, paragrafi 1 e 2, in relazione al paese designato che desta preoccupazioni per la cibersicurezza delle catene di approvvigionamento delle TIC in cui il soggetto è stabilito o dal quale è controllato;
 - b) l'efficacia delle misure di attenuazione di cui al paragrafo 2, lettera b);
 - c) il fatto che l'esenzione per il soggetto stabilito in un paese terzo che desta preoccupazioni per la cibersicurezza delle catene di approvvigionamento delle TIC, oppure controllato da soggetti di tale paese terzo, non sarebbe lesiva degli interessi dell'Unione.

5. Se conclude, a seguito della valutazione di cui al paragrafo 3, che la concessione di un'esenzione è giustificata, la Commissione procede in tal senso mediante una decisione notificata al richiedente entro nove mesi dal ricevimento della richiesta.
6. Nell'adottare una decisione di cui al paragrafo 4, la Commissione può limitare l'esenzione a un determinato periodo di tempo e subordinarne la concessione a talune condizioni cui il soggetto deve attenersi, ossia:
 - a) un calendario per l'attuazione delle misure di attenuazione di cui al paragrafo 2, lettera b);
 - b) audit periodici da parte di terzi per garantire l'efficace attuazione delle misure di attenuazione;
 - c) obblighi di comunicazione per quanto riguarda la conformità.
7. Se conclude, a seguito della valutazione di cui al paragrafo 3, che la concessione di un'esenzione non è giustificata, la Commissione procede di conseguenza mediante una decisione notificata ai richiedenti entro nove mesi dal ricevimento della richiesta.
8. La Commissione può, di propria iniziativa, revocare o modificare la decisione di cui al paragrafo 4 in una o più delle situazioni seguenti:
 - a) si è verificato un cambiamento sostanziale dei fatti su cui si basava la decisione;
 - b) il soggetto che ha richiesto l'esenzione contravviene agli impegni assunti;
 - c) l'esenzione si basava su informazioni incomplete, inesatte o fuorvianti fornite dal soggetto che ha presentato la richiesta.

Articolo 106 *Diritti della difesa*

La Commissione provvede affinché, prima di adottare un atto di esecuzione a norma dell'articolo 103, paragrafo 7, o prima di adottare la decisione di non concedere l'esenzione a norma dell'articolo 105, paragrafo 7, sulla base della mancata presentazione di elementi da parte del richiedente, o prima di revocare una decisione a norma dell'articolo 105, paragrafo 8, al soggetto interessato sia data la possibilità di essere ascoltato, tenendo conto della necessità, in alcuni casi, di ricorrere a una procedura d'urgenza.

Articolo 107 *Registro*

La Commissione tiene un registro accessibile al pubblico delle decisioni adottate a norma dell'articolo 105, paragrafo 5. Il registro riporta i nomi dei soggetti destinatari di tali decisioni. La Commissione aggiorna il registro periodicamente.

Articolo 108 *Riservatezza*

Le informazioni ricevute dalla Commissione a norma degli articoli 105 e 106 sono utilizzate solo per la finalità per la quale sono state acquisite.

Articolo 109

Diritti

1. La Commissione riscuote diritti per le richieste presentate in conformità dell'articolo 105, paragrafo 1.
2. I diritti sono espressi e riscossi in euro.
3. I diritti sono commisurati ai costi connessi al trattamento delle richieste di cui all'articolo 105, paragrafo 1, alla valutazione dei criteri e delle informazioni di cui all'articolo 105, paragrafo 2, e alla creazione, al mantenimento e alla gestione del registro di cui all'articolo 107. Rientrano in tali costi tutte le spese per il personale impegnato in tali attività sostenute dalla Commissione.
4. La Commissione adotta atti di esecuzione che stabiliscono norme dettagliate relative ai diritti, specificandone l'importo e le modalità di pagamento. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.

Capo II

Catene di approvvigionamento delle TIC nelle reti di comunicazione elettronica

Articolo 110

Risorse TIC chiave per le reti di comunicazione elettronica mobili, fisse e satellitari

1. Le risorse TIC chiave per le reti di comunicazione elettronica mobili, fisse e satellitari figurano nell'allegato II.
2. I componenti TIC o i componenti che comprendono componenti TIC forniti da fornitori ad alto rischio sono gradualmente eliminati dalle risorse TIC chiave delle reti di comunicazione elettronica mobili, fisse e satellitari.
3. Il termine per l'eliminazione graduale dei componenti TIC o dei componenti che comprendono componenti TIC forniti da fornitori ad alto rischio per quanto riguarda le reti di comunicazione elettronica mobili non supera i 36 mesi dalla pubblicazione dell'elenco dei fornitori ad alto rischio di cui all'articolo 104 pertinenti alle reti di comunicazione elettronica mobili.
4. Alla Commissione è conferito il potere di adottare atti di esecuzione conformemente all'articolo 118, paragrafo 2, per specificare i termini per l'eliminazione graduale dei componenti TIC o dei componenti che comprendono componenti TIC forniti da fornitori ad alto rischio per quanto riguarda le reti di comunicazione elettronica fisse e satellitari.
5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 119 per modificare l'allegato II del presente regolamento in modo da adeguarlo agli sviluppi tecnologici tenendo conto degli elementi di cui all'articolo 103, paragrafo 4.

Articolo 111

Divieti per le reti di comunicazione elettronica mobili, fisse e satellitari

1. I fornitori di reti di comunicazione elettronica mobili, fisse e satellitari non utilizzano, installano o integrano, in alcuna forma, componenti TIC o componenti che comprendono componenti TIC di fornitori ad alto rischio nell'ambito delle risorse TIC chiave di cui all'allegato II.

2. Se l'autorità competente designata a norma del presente regolamento in uno Stato membro differisce dall'autorità competente a norma del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali], l'autorità competente designata a norma del presente regolamento informa senza indugio l'autorità competente a norma del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali] in merito alle misure imposte ai fornitori di reti di comunicazione elettronica mobili, fisse e satellitari in conformità dell'articolo 114. Le autorità assicurano una stretta cooperazione ai fini di una vigilanza e di un'esecuzione efficaci di tali misure.

Capo III

Autorità competenti, vigilanza ed esecuzione, giurisdizione, diritti della difesa

Articolo 112

Autorità competenti

1. Ciascuno Stato membro designa le autorità competenti di cui all'articolo 8 della direttiva (UE) 2022/2555 quali autorità responsabili dell'adozione delle misure di vigilanza e di esecuzione di cui all'articolo 114.
2. Le autorità competenti sono pienamente imparziali, a livello strutturale e funzionale, e non subiscono alcuna influenza esterna, diretta o indiretta; in particolare non sollecitano né accettano istruzioni da altre autorità pubbliche o da privati.
3. Gli Stati membri provvedono affinché le loro autorità competenti dispongano dei poteri adeguati, delle risorse umane e tecniche sufficienti e delle competenze necessarie per attuare efficacemente le misure di vigilanza e di esecuzione di cui all'articolo 114.
4. Ciascuno Stato membro notifica senza indebito ritardo alla Commissione i nomi delle autorità competenti designate a norma del paragrafo 1, i compiti rispettivi di tali autorità e qualsiasi successiva modifica degli stessi. Ciascuno Stato membro rende inoltre pubblici i nomi delle autorità competenti designate a norma del paragrafo 1.

Articolo 113

Rete dei servizi di cooperazione e di sostegno della Commissione

Ai fini di una vigilanza efficace, la Commissione istituisce una rete di cooperazione tra le autorità competenti degli Stati membri di cui all'articolo 112 e la Commissione; tale rete funge da piattaforma per la cooperazione e lo scambio di informazioni, in particolare ai fini della valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo di cui all'articolo 104. La Commissione fornisce alla rete sostegno amministrativo.

Articolo 114

Misure di vigilanza e di esecuzione

1. Le autorità competenti di cui all'articolo 112 sono autorizzate ad adottare le misure di vigilanza e di esecuzione nei confronti dei soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555. Gli Stati membri provvedono affinché le suddette misure siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso. Gli Stati membri notificano alla Commissione le norme adottate a tal fine e le loro successive modifiche.

2. Nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555, le autorità competenti hanno il potere di sottoporre tali soggetti a:
 - a) richieste di invio di un elenco dettagliato e aggiornato dei loro fornitori e prestatori di servizi pertinenti;
 - b) richieste di accesso a dati, documenti e informazioni necessari per verificare la conformità al presente regolamento;
 - c) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
 - d) richieste riguardanti la composizione dei prodotti hardware o software installati o integrati in qualsiasi forma nella rete o nel sistema, compresi i componenti e le dipendenze transitive, in un formato di uso comune e leggibile da un dispositivo automatico.
3. Nell'esercizio delle rispettive competenze di esecuzione nei confronti dei soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555, le autorità competenti hanno il potere di:
 - a) emanare avvertimenti relativi a violazioni del presente regolamento da parte dei soggetti interessati, esponendo i fatti e le considerazioni giuridiche pertinenti;
 - b) adottare decisioni che impongono ai soggetti interessati di porre rimedio alla violazione del presente regolamento o alle carenze individuate nell'attuazione delle misure di attenuazione;
 - c) imporre ai soggetti interessati di porre fine alle attività che violano il presente regolamento e di astenersi dal ripeterle; e
 - d) imporre sanzioni, conformemente alle disposizioni relative all'importo di cui all'articolo 115, o chiedere l'imposizione di tali sanzioni da parte degli organismi o degli organi giurisdizionali pertinenti, conformemente al diritto nazionale.
4. Nell'adottare qualsiasi delle misure di esecuzione di cui al paragrafo precedente, le autorità competenti considerano le circostanze di ciascun singolo caso e tengono debitamente conto dei fattori seguenti:
 - a) la gravità della violazione e l'importanza delle disposizioni violate;
 - b) la durata della violazione;
 - c) il fatturato del soggetto interessato;
 - d) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;
 - e) ove applicabile, qualsiasi danno materiale o immateriale causato dalla violazione, incluse le perdite finanziarie o economiche, gli effetti su altri soggetti e il numero di utenti interessati;
 - f) un'eventuale condotta intenzionale o negligente da parte del soggetto interessato;
 - g) qualsiasi misura adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale;

- h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti.

Ai fini del primo comma, lettera a), sono da considerarsi violazioni gravi:

- i) le violazioni ripetute;
 - j) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;
 - k) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti.
5. Prima di adottare misure di esecuzione, le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Ai soggetti interessati è concesso un tempo ragionevole per presentare osservazioni sulle conclusioni preliminari. Le autorità competenti espongono nei particolari la motivazione delle loro misure di esecuzione.
 6. Le autorità competenti rispettano il principio di riservatezza e il principio del segreto professionale e commerciale.
 7. Le autorità competenti cooperano tra loro e con la Commissione a fini di vigilanza ed esecuzione a norma del presente titolo conformemente all'articolo 116.

Articolo 115

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni da applicare in caso di violazione del presente regolamento e adottano tutte le misure necessarie per assicurarne l'applicazione.
2. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.
3. Le sanzioni sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 114, paragrafo 3, lettere a), b) e c).
4. Nel decidere se imporre una sanzione e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno dei fattori di cui all'articolo 114, paragrafo 4, primo comma.
5. Le violazioni dell'articolo 103, paragrafo 2, lettera a), sono soggette, conformemente al paragrafo 3 del presente articolo, a sanzioni pari a un massimo dell'1 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa a cui il soggetto appartiene.
6. Le violazioni dell'articolo 103, paragrafo 2, lettere da b) a g), sono soggette, conformemente al paragrafo 3 del presente articolo, a sanzioni pari a un massimo del 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa a cui il soggetto appartiene.
7. Le violazioni dell'articolo 103, paragrafo 1, e dell'articolo 111 sono soggette, conformemente al paragrafo 3 del presente articolo, a sanzioni pari a un massimo del 7 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa a cui il soggetto appartiene.

Articolo 116
Assistenza reciproca

1. Se un soggetto del tipo di cui all'allegato I o II della direttiva (UE) 2022/2555 fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e le sue risorse TIC chiave sono ubicate in uno o più altri Stati membri, le autorità competenti degli Stati membri interessati cooperano tra loro e con la Commissione, si prestano assistenza reciproca e assistono la Commissione al fine di garantire l'applicazione efficace ed efficiente del regolamento. A tal fine si applicano almeno le seguenti regole:
 - a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate;
 - b) un'autorità competente di uno Stato membro può chiedere a un'altra autorità competente di un altro Stato membro di adottare misure di vigilanza o esecuzione;
 - c) un'autorità competente di uno Stato membro, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente di un altro Stato membro, fornisce a tale altra autorità competente un'assistenza reciproca con la massima diligenza possibile affinché le misure di vigilanza o esecuzione possano essere attuate in maniera efficace, efficiente e coerente.
2. L'assistenza reciproca di cui al paragrafo 1, lettera c), può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione.
3. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza congiunte.
4. In considerazione dell'obbligo di rispettare il principio di riservatezza e il principio del segreto professionale e commerciale di cui all'articolo 114, paragrafo 6, le informazioni scambiate nell'ambito di una richiesta di assistenza e fornite a norma del presente articolo sono utilizzate soltanto in relazione alla questione per la quale sono state richieste.

Articolo 117
Giurisdizione e territorialità

1. I soggetti di un tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 che rientrano nell'ambito di applicazione del presente regolamento sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:

- a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;
 - b) i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione a norma del paragrafo 2;
 - c) gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro a cui appartengono;
 - d) i vettori aerei, che sono considerati sotto la giurisdizione dello Stato membro la cui autorità competente per il rilascio delle licenze ha rilasciato al soggetto la licenza di esercizio a norma del regolamento (CE) n. 1008/2008 del Parlamento europeo e del Consiglio⁸³ oppure, se la licenza di esercizio o altro documento equivalente non è stato rilasciato a norma di detto regolamento, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno il proprio stabilimento principale nell'Unione a norma del paragrafo 2.
2. Ai fini del presente regolamento, si considera che un soggetto di cui al paragrafo 1, lettera b), abbia il proprio stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui sono effettuate la maggior parte delle operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione.
3. Se un soggetto di cui agli allegati I e II della direttiva (UE) 2022/2555 non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Qualora si tratti di un soggetto di cui al paragrafo 1, lettera a), tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui presta i suoi servizi. Nell'assenza di un rappresentante nell'Unione designato a norma del presente paragrafo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per violazione degli obblighi del presente regolamento.
4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.
5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un soggetto di cui al paragrafo 1, lettera b), possono, entro i limiti della richiesta,

⁸³ Regolamento (CE) n. 1008/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, recante norme comuni per la prestazione di servizi aerei nella Comunità (rifusione) (GU L 293 del 31.10.2008, pag. 3, ELI: <http://data.europa.eu/eli/reg/2008/1008/oj>).

adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato se il soggetto fornisce servizi o ha un sistema informativo e di rete nel loro territorio.

Titolo VI

Disposizioni finali

Articolo 118

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso si riunisce in due formazioni. Per quanto riguarda i titoli II e III, la Commissione è assistita dal comitato riunito nella prima formazione; per quanto riguarda il titolo IV la Commissione è invece assistita dal comitato riunito nella seconda formazione. 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 119

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 80, paragrafo 2, e all'articolo 110, paragrafo 5, è conferito alla Commissione per un periodo indeterminato a decorrere dalla data di entrata in vigore del presente regolamento.
3. La delega di potere di cui di cui all'articolo 80, paragrafo 2, e all'articolo 110, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.
5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
6. L'atto delegato adottato a norma dell'articolo 80, paragrafo 2, e dell'articolo 110, paragrafo 5, 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 120
Valutazione e riesame

1. Entro il [GG MM AAAA], e successivamente ogni cinque anni, la Commissione fa eseguire una valutazione che è svolta conformemente agli orientamenti da essa emanati.
2. La valutazione di cui al paragrafo 1 esamina:
 - a) le prestazioni dell'ENISA in relazione ai suoi obiettivi, al suo mandato, alla sua missione, ai suoi compiti, alla sua governance e alla sua ubicazione;
 - b) l'efficacia, l'efficienza e il valore aggiunto dell'UE dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza di cui al titolo II, capo II, sezione 4, del presente regolamento;
 - c) l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e dei soggetti dell'Unione e di migliorare il funzionamento del mercato interno;
 - d) l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo IV del presente regolamento per quanto riguarda gli obiettivi del quadro affidabile per le catene di approvvigionamento delle TIC.
3. La valutazione di cui al paragrafo 1, lettera a), esamina in particolare l'eventuale necessità di modificare il mandato dell'ENISA e le conseguenti implicazioni finanziarie.
4. Ogni due valutazioni di cui al paragrafo 1, lettera a), la Commissione esamina i risultati conseguiti dall'ENISA, tenuto conto degli obiettivi, del mandato, della missione, della governance e dei compiti dell'Agenzia, valutando altresì se il mantenimento dell'ENISA sia ancora giustificato alla luce di tali obiettivi, mandato, missione, governance e compiti.
5. La Commissione riferisce al Parlamento europeo, al Consiglio e al consiglio di amministrazione sui risultati della valutazione. I risultati della valutazione sono resi pubblici.

Articolo 121
Abrogazione e prosecuzione delle attività

1. Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio è abrogato con effetto a decorrere dal GGMMAAAA.
2. I riferimenti al regolamento (UE) 2019/881, all'ENISA e ai sistemi europei di certificazione della cibersicurezza istituiti da tale regolamento si intendono fatti al presente regolamento e si leggono secondo la tavola di concordanza di cui all'allegato III del presente regolamento.
3. L'ENISA disciplinata dal presente regolamento prosegue l'operato e le attività dell'ENISA istituita dal regolamento (UE) 2019/881 per quanto riguarda diritti di proprietà, accordi, obblighi di legge, contratti di lavoro, impegni finanziari e responsabilità. Tutte le decisioni del consiglio di amministrazione e del comitato esecutivo adottate a norma del regolamento (UE) 2019/881 restano valide, purché siano conformi al presente regolamento.

4. Il direttore esecutivo nominato a norma dell'articolo 15, paragrafo 1, lettera n), del regolamento (UE) 2019/881 resta in carica ed assolve i compiti e le responsabilità del direttore esecutivo ai sensi dell'articolo 32 del presente regolamento per la restante durata del mandato. Le altre condizioni contrattuali rimangono invariate.
5. Le proposte di sistemi la cui preparazione è stata richiesta a norma dell'articolo 49 del regolamento (UE) 2019/881 si considerano richieste a norma delle corrispondenti disposizioni del presente regolamento. Le disposizioni del titolo III del presente regolamento si applicano di conseguenza a tali proposte di sistemi.
6. I membri del consiglio di amministrazione nominati dalla Commissione e i membri supplenti nominati a norma dell'articolo 14 del regolamento (UE) 2019/881 restano in carica ed esercitano le funzioni del consiglio di amministrazione ai sensi dell'articolo 27 del presente regolamento per la restante durata del mandato. I membri del consiglio di amministrazione nominati dagli Stati membri a norma dell'articolo 14 del regolamento (UE) 2019/881 restano in carica ed esercitano le funzioni del consiglio di amministrazione ai sensi dell'articolo 27 del presente regolamento, a condizione che esercitino le funzioni di cui all'articolo 24, paragrafo 3, del presente regolamento.

Articolo 122
Entrata in vigore

Il presente regolamento entra in vigore il [...] 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 Strasburgo, il

Per il Parlamento europeo
La presidente

Per il Consiglio
Il presidente

SCHEDA FINANZIARIA E DIGITALE LEGISLATIVA

1.	CONTESTO DELLA PROPOSTA/INIZIATIVA	3
1.1.	Titolo della proposta/iniziativa	3
1.2.	Settore/settori interessati	3
1.3.	Obiettivi	3
1.3.1.	Obiettivi generali.....	3
1.3.2.	Obiettivi specifici	3
1.3.3.	Risultati e incidenza previsti	3
1.3.4.	Indicatori di prestazione	3
1.4.	La proposta/iniziativa riguarda:	4
1.5.	Motivazione della proposta/iniziativa	4
1.5.1.	Necessità nel breve e lungo termine, con calendario dettagliato delle fasi di attuazione dell'iniziativa.....	4
1.5.2.	Valore aggiunto dell'intervento dell'UE (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini della presente sezione, per "valore aggiunto dell'intervento dell'UE" si intende il valore derivante dall'azione dell'Unione europea che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.	4
1.5.3.	Insegnamenti tratti da esperienze analoghe.....	4
1.5.4.	Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti rilevanti	5
1.5.5.	Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione	5
1.6.	Durata della proposta/iniziativa e della relativa incidenza finanziaria	6
1.7.	Metodo o metodi di esecuzione del bilancio previsti.....	6
2.	MISURE DI GESTIONE	8
2.1.	Disposizioni in materia di monitoraggio e di relazioni	8
2.2.	Sistema o sistemi di gestione e di controllo	8
2.2.1.	Giustificazione del metodo o dei metodi di esecuzione del bilancio, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti.....	8
2.2.2.	Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli	8
2.2.3.	Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto tra costi del controllo e valore dei fondi gestiti) e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura).....	8
2.3.	Misure di prevenzione delle frodi e delle irregolarità.....	9
3.	INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA.....	10

3.1.	Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate.....	10
3.2.	Incidenza finanziaria prevista della proposta sugli stanziamenti.....	12
3.2.1.	Sintesi dell'incidenza prevista sugli stanziamenti operativi.....	12
3.2.1.1.	Stanziamenti dal bilancio votato.....	12
3.2.1.2.	Stanziamenti da entrate con destinazione specifica esterne.....	17
3.2.2.	Risultati previsti finanziati con gli stanziamenti operativi.....	22
3.2.3.	Sintesi dell'incidenza prevista sugli stanziamenti amministrativi.....	24
3.2.3.1.	Stanziamenti dal bilancio votato.....	24
3.2.3.2.	Stanziamenti da entrate con destinazione specifica esterne.....	24
3.2.3.3.	Totale degli stanziamenti.....	24
3.2.4.	Fabbisogno previsto di risorse umane.....	25
3.2.4.1.	Finanziamento a titolo del bilancio votato.....	25
3.2.4.2.	Finanziamento a titolo di entrate con destinazione specifica esterne.....	26
3.2.4.3.	Fabbisogno totale di risorse umane.....	26
3.2.5.	Panoramica dell'incidenza prevista sugli investimenti connessi a tecnologie digitali.....	28
3.2.6.	Compatibilità con il quadro finanziario pluriennale attuale.....	28
3.2.7.	Partecipazione di terzi al finanziamento.....	28
3.3.	Incidenza prevista sulle entrate.....	29
4.	DIMENSIONI DIGITALI.....	29
4.1.	Prescrizioni di rilevanza digitale.....	30
4.2.	Dati.....	30
4.3.	Soluzioni digitali.....	31
4.4.	Valutazione dell'interoperabilità.....	31
4.5.	Misure a sostegno dell'attuazione digitale.....	32

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")

(Testo rilevante ai fini del SEE)

Titolo abbreviato: regolamento sulla cibersicurezza 2

e

proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2]

1.2. Settore/settori interessati

Settore: 09 – Reti di comunicazione, contenuti e tecnologie

Attività: 09.02 Mercato unico digitale

1.3. Obiettivi

1.3.1. Obiettivi generali

Gli obiettivi principali dell'intervento sono:

1) Rafforzare le capacità e la resilienza in materia di cibersicurezza:

contribuire a rafforzare la governance della cibersicurezza dell'Unione e a garantire che le istituzioni, le autorità e gli altri pertinenti portatori di interessi siano meglio preparati a prevenire, rilevare e rispondere alle minacce alla cibersicurezza in modo coordinato ed efficace.

2) Prevenire la frammentazione nel mercato interno:

sostenere l'elaborazione, l'attuazione e l'adozione di strumenti comuni dell'Unione in materia di cibersicurezza, quali sistemi di certificazione, e fornire quadri armonizzati che rafforzino la fiducia e l'interoperabilità tra gli Stati membri.

Questi obiettivi generali rispondono alle principali sfide individuate in fase di definizione del problema nella valutazione d'impatto dell'iniziativa proposta e rispecchiano l'obiettivo strategico generale di rafforzare la governance della cibersicurezza nell'Unione e di sostenere lo sviluppo di un mercato unico digitale sicuro, resiliente e competitivo.

1.3.2. Obiettivi specifici

Per affrontare il disallineamento tra il quadro strategico dell'UE in materia di cibersicurezza e le esigenze dei portatori di interessi:

Obiettivo specifico n. 1: creare la capacità di attuare efficacemente le politiche dell'Unione in materia di cibersicurezza e una cooperazione operativa continua che consenta una cooperazione più strutturata tra gli Stati membri.

Obiettivo specifico n. 2: sviluppare e applicare i mezzi e i meccanismi per sostenere e rispondere efficacemente alle esigenze degli Stati membri, dell'industria e di altri portatori di interessi.

Per far fronte alla scarsa diffusione e alla limitata efficacia del quadro europeo di certificazione della cibersicurezza:

Obiettivo specifico n. 3: creare i presupposti per una più rapida attuazione dei sistemi di certificazione della cibersicurezza sulla base delle esigenze del mercato, ampliando l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza, garantendo un mantenimento efficace e procedure agili e aumentando la trasparenza.

Per affrontare la frammentarietà del panorama della conformità e la complessità dei quadri orizzontali e settoriali:

Obiettivo specifico n. 4: creare meccanismi e condizioni per agevolare la conformità ai requisiti di cibersicurezza, rendendo in tal modo la loro attuazione più coerente ed efficace.

Per affrontare i rischi di cibersicurezza nella catena di approvvigionamento:

Obiettivo specifico n. 5: ridurre i rischi per le catene di approvvigionamento critiche delle TIC provenienti da soggetti stabiliti in paesi che destano preoccupazioni per la cibersicurezza o controllati da soggetti di tali paesi (fornitori ad alto rischio) e ridurre le dipendenze critiche sviluppando un quadro coerente ed efficace a livello dell'UE per affrontare i rischi per la sicurezza delle catene di approvvigionamento delle TIC.

1.3.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Risultati previsti:

- 1) Riforma funzionale dell'ENISA
- 2) Riforma del quadro europeo di certificazione della cibersicurezza – ampliamento dell'ambito di applicazione, nuova procedura e governance riveduta
- 3) Ulteriore semplificazione della conformità al pertinente quadro normativo dell'Unione in materia di cibersicurezza
- 4) Quadro globale e orizzontale per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC

Impatto complessivo:

La proposta avrà un enorme impatto sulla cibersicurezza nell'Unione in quanto affronta una serie di aspetti come la necessità di rafforzare l'Agenzia dell'Unione europea per la cibersicurezza, rafforza il sostegno all'attuazione del diritto dell'UE, introduce riforme per un'attuazione agevole del quadro europeo di certificazione, promuove una comprensione comune, a livello dell'Unione, delle minacce informatiche e affronta l'attenuazione dei rischi di cibersicurezza in funzione del contesto geopolitico. L'attuazione delle disposizioni proposte garantirà livelli elevati di efficienza e coerenza ed eviterà oneri normativi eccessivi. Il pacchetto è strutturato in modo tale da essere resiliente alle sfide legate all'attuazione e da garantire la coerenza a lungo termine delle politiche in tutto l'ecosistema digitale e della cibersicurezza. Esso migliora la chiarezza, eliminando le inefficienze e allineando le procedure tra i quadri giuridici, e nel contempo contribuisce al conseguimento di un

livello elevato di cibersicurezza in tutta l'UE. Poiché la semplificazione è uno dei principali obiettivi prioritari della Commissione europea, gli sforzi previsti in tal senso produrranno notevoli vantaggi economici, quantificati in oltre 14,63 miliardi di EUR per le imprese, comprese le PMI, e in 7,5 milioni di EUR per le autorità pubbliche.

Risultati specifici:

- aumentare la consapevolezza e migliorare il coordinamento operativo, il che potrebbe generare notevoli risparmi sui costi per le imprese, le autorità pubbliche e i cittadini grazie a una maggiore rapidità di rilevazione degli incidenti e di risposta agli stessi;
- chiarire l'ambito di intervento e le competenze dell'ENISA, garantendo nel contempo la necessaria definizione delle priorità per quanto riguarda i suoi compiti principali;
- garantire che i portatori di interessi ricevano un sostegno adeguato per l'attuazione delle politiche, le attività operative e il coordinamento generale;
- promuovere la conoscenza situazionale condivisa dell'Unione;
- rafforzare la cooperazione con EU-CyCLONe, la rete di CSIRT, la Commissione, Europol, il CERT-UE e i pertinenti soggetti dell'Unione al fine di sviluppare archivi di intelligence verificata e affidabile sulle minacce informatiche;
- sostenere gli sforzi volti ad attenuare gli attacchi ransomware;
- rafforzare il coordinamento con il settore privato su temi connessi alla cibersicurezza;
- diffondere informazioni tempestive attraverso allerte precoci riguardanti incidenti significativi o su vasta scala o minacce informatiche di natura transfrontaliera, in relazione ai settori elencati negli allegati I e II della direttiva (UE) 2022/2555;
- promuovere sinergie efficaci con altri organi e organismi dell'UE;
- ridurre il prezzo delle certificazioni delle competenze, anche aumentando l'offerta sul mercato mediante l'introduzione dei sistemi europei di attestazione delle competenze;
- contribuire a eliminare il divario di competenze in Europa attraverso attestati delle competenze individuali in materia di cibersicurezza e sostenere gli Stati membri e l'industria nel rafforzamento della propria forza lavoro;
- rimediare alla scarsa chiarezza del quadro europeo di certificazione della cibersicurezza e al suo impatto limitato, ampliandone l'ambito di applicazione e migliorandone il modello di governance;
- accrescere la reputazione dei sistemi adottati attraverso la creazione di una struttura di mantenimento e l'introduzione di un processo di sviluppo tempestivo e trasparente;
- introdurre un meccanismo di riscossione di diritti in relazione ai costi sostenuti per lo sviluppo e il mantenimento dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza e per il trattamento delle domande e la concessione di autorizzazioni ai fornitori, nonché per il

mantenimento dei sistemi adottati nell'ambito del quadro europeo di certificazione della cibersecurity, il che contribuirà alla stabilità finanziaria dell'Agenzia e permetterà di realizzare risparmi nell'ambito del bilancio dell'UE;

- allineare i sistemi europei di certificazione al quadro legislativo esistente e in tal modo sostenere maggiormente gli sforzi di attuazione e rispondere meglio alle esigenze delle imprese in materia di conformità;
- consentire l'adozione di sistemi attualmente bloccati;
- favorire la competitività delle imprese europee promuovendo l'allineamento tra le norme internazionali e quelle europee;
- limitare la frammentazione delle misure e dei requisiti di cibersecurity;
- assicurare chiarezza giuridica e ridurre in misura sostanziale gli oneri amministrativi, senza generare una notevole incertezza giuridica tra i portatori di interessi che si stanno adeguando ai quadri giuridici di recente adozione;
- agevolare la conformità per i soggetti rientranti nell'ambito di applicazione della direttiva NIS 2, il che contribuirebbe anche al miglioramento del tasso di conformità complessivo e alla messa in atto di misure più incisive in materia di cibersecurity, incrementando al contempo l'efficienza del processo di vigilanza da parte delle autorità.

Altro

- L'iniziativa produrrebbe numerosi effetti positivi sulle PMI, considerando il miglioramento della competitività all'interno del mercato della cibersecurity dell'UE e la riduzione dei costi e degli oneri amministrativi:
 1. *ruolo positivo per quanto riguarda le PMI, che trarrebbero vantaggio da una maggiore ciberresilienza resa possibile dal ruolo rafforzato dell'ENISA e dagli orientamenti tecnici forniti dall'Agenzia;*
 2. *le PMI, in quanto fornitori autorizzati a rilasciare attestati nell'ambito del sistema europeo di attestazione delle competenze, avranno maggiore visibilità, godranno di una migliore reputazione e acquisiranno nuovi clienti. Inoltre gli attestati europei delle competenze individuali in materia di cibersecurity aiuteranno le PMI a individuare i candidati con le giuste competenze;*
 3. *sistemi europei di certificazione ben funzionanti possono agevolare la scelta di tecnologie TIC affidabili per le PMI e contribuire a rafforzare la loro ciberresilienza complessiva;*
 4. *in quanto fornitori di servizi DNS, le PMI beneficeranno di misure relative all'attuazione della direttiva NIS 2 grazie alle esclusioni dei fornitori di servizi DNS dall'ambito di applicazione;*
 5. *le PMI trarrebbero vantaggio dai chiarimenti forniti in merito all'ambito di applicazione, che limiterebbero l'applicazione degli obblighi a determinati soggetti in alcuni settori elencati nella direttiva NIS 2;*
 6. *per le misure relative alla sicurezza delle catene di approvvigionamento delle TIC, le PMI in generale trarrebbero vantaggio dall'uso di tecnologie affidabili. Poiché tali imprese operano come fornitori nei settori soggetti a restrizioni, i costi di sostituzione e di transazione inciderebbero su di esse in misura maggiore che non sulle imprese più grandi. Tuttavia le PMI, in quanto fornitori affidabili, beneficeranno di nuove opportunità di mercato.*

- Non si prevede un impatto ambientale significativo per nessuno degli obiettivi fissati.
- Per quanto riguarda il bilancio dell'UE, è possibile conseguire una maggiore efficienza rafforzando la cooperazione e il coordinamento delle attività tra istituzioni, organi e organismi dell'UE. Si prevedono risparmi nel lungo periodo grazie all'introduzione di meccanismi di riscossione di diritti.

1.3.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati

Obiettivo: creare la capacità di attuare efficacemente le politiche dell'UE in materia di cbersicurezza e una cooperazione operativa regolare/continua che consenta una cooperazione più strutturata tra gli Stati membri.

- *Numero di contributi pertinenti dell'ENISA all'attuazione delle politiche e delle iniziative legislative dell'UE e nazionali*

- *Riscontri positivi da parte dei portatori di interessi per quanto riguarda i pertinenti contributi dell'ENISA*

- *Aumento del 25 % rispetto al valore di riferimento del 2023 indicato nella relazione annuale di attività dell'ENISA (numero di contributi pertinenti) e nell'indagine annuale dell'ENISA sul grado di soddisfazione (riscontri positivi)*

- *Statistiche sull'uso della banca dati europea delle vulnerabilità*

- *Aumento del 25 % del numero di utenti rispetto al 2025*

Disponibilità, sicurezza e funzionamento della piattaforma istituita dal regolamento sulla ciberresilienza

- *Diminuzione del 25 % dei tempi di inattività della piattaforma e del numero di incidenti rispetto alle statistiche del 2025 riguardanti i tempi di inattività e gli incidenti sulla piattaforma*

Obiettivo: sviluppare e attuare i mezzi e i meccanismi per fornire sostegno e rispondere efficacemente alle esigenze degli Stati membri, dell'industria e di altri portatori di interessi.

- *Numero di portatori di interessi sostenuti dall'ENISA e qualità del sostegno fornito*

- *Numero di misure attuate a sostegno dei portatori di interessi*

- *Aumento del 10 % del numero di portatori di interessi che beneficiano del sostegno e aumento del 10 % del loro livello di soddisfazione rispetto al 2025*

Obiettivo: creare i presupposti per una più rapida attuazione dei sistemi di certificazione della cbersicurezza sulla base delle esigenze del mercato, ampliando l'ambito di applicazione del quadro europeo di certificazione della cbersicurezza, garantendo un mantenimento efficace e procedure agili e migliorando la trasparenza.

- *Numero di sistemi adottati*

- *Riduzione del 50 % dei tempi necessari per lo sviluppo di un sistema rispetto al 2025*
- *Numero di certificati validi rilasciati ogni anno*
- *Aumento del 25 % rispetto al valore di riferimento del 2025*
- *Riscontri positivi dei portatori di interessi per quanto riguarda la loro partecipazione allo sviluppo dei sistemi e la trasparenza del quadro europeo di certificazione della cibersecurity*
- *Aumento del 25 % rispetto al valore di riferimento nell'indagine annuale dell'ENISA sul grado di soddisfazione (rispetto al 2027)*

Obiettivo: definire meccanismi e condizioni per contribuire ad agevolare la conformità ai requisiti di cibersecurity, aumentando in tal modo la coerenza e l'efficacia della loro attuazione.

- *Costi sostenuti dalle PMI per conformarsi alla direttiva NIS 2 e alle norme in materia di cibersecurity, in percentuale di tutti i costi di conformità*
- *Più del 70 % delle PMI segnala una riduzione dei costi di conformità per la cibersecurity rispetto al 2025*
- *Numero di attacchi ransomware e importo dei risarcimenti in EUR*
- *Riduzione del numero di attacchi ransomware > 1 % rispetto al 2027*
- *Percentuale di incidenti transfrontalieri durante o dopo i quali le autorità degli Stati membri hanno fatto ricorso a meccanismi di assistenza reciproca*
- *Aumento di oltre 20 punti percentuali, rispetto al 2025, dei casi in cui si è fatto ricorso all'assistenza reciproca*

Obiettivo: ridurre le dipendenze critiche sviluppando un quadro coerente ed efficace a livello dell'UE per affrontare i rischi per la sicurezza delle catene di approvvigionamento delle TIC.

- *Numero di misure adottate*
- *Aumento del 25 % del numero di misure adottate e delle risorse chiave individuate rispetto alla data di adozione + 6 mesi*
- *Diminuzione del 25 %, rispetto al 2025, delle dipendenze da fornitori ad alto rischio per quanto riguarda le risorse TIC chiave*

1.4. La proposta/iniziativa riguarda:

- ☒ una nuova azione (Titolo IV - Catena di approvvigionamento, titolo V - Semplificazione)
- ☐ una nuova azione a seguito di un progetto pilota/un'azione preparatoria⁸⁴;

⁸⁴

A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

☒ la proroga di un'azione esistente (*Titolo II - Mandato dell'ENISA, e titolo III - Certificazione*)

☐ la fusione o il riorientamento di una o più azioni verso un'altra/una nuova azione.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, con calendario dettagliato delle fasi di attuazione dell'iniziativa

Nel luglio 2024, nei suoi orientamenti politici⁸⁵, la presidente della Commissione europea Ursula von der Leyen ha chiesto di semplificare, consolidare e codificare la normativa dell'UE, al fine di eliminare le eventuali sovrapposizioni e contraddizioni mantenendo nel contempo standard elevati. La lettera d'incarico alla vicepresidente esecutiva Virkkunen⁸⁶ menziona in particolare il miglioramento del processo di adozione dei sistemi europei di certificazione della cibersecurity e la necessità di proteggere le industrie, i cittadini e le pubbliche amministrazioni dell'UE da minacce interne ed esterne. Inoltre la relazione Niinistö del 2024⁸⁷ invita a ridurre il rischio di dipendenze indesiderate nelle catene di approvvigionamento per quanto riguarda le tecnologie critiche. Le relazioni Draghi⁸⁸ e Letta⁸⁹, commissionate dalla presidente dell'UE, hanno soprattutto evidenziato la necessità di far sì che il mercato unico rimanga competitivo attraverso la semplificazione e garantisca i massimi livelli di sicurezza e di autonomia strategica. Partendo da tale presupposto, la revisione del regolamento sulla cibersecurity è una pietra angolare del lavoro svolto dalla Commissione nel settore della sicurezza e introduce una revisione ambiziosa dell'ecosistema normativo europeo in materia di cibersecurity. La proposta relativa al regolamento sulla cibersecurity 2 introduce meccanismi per affrontare i rischi di cibersecurity nella catena di approvvigionamento e meccanismi per ridurre la frammentazione del panorama della conformità e la complessità dei quadri orizzontali e settoriali. Si prevede che anche l'ENISA contribuirà a semplificare ulteriormente gli obblighi di comunicazione attraverso l'integrazione di un punto di accesso unico.

Inoltre, in considerazione del numero di disposizioni settoriali introdotte dopo l'adozione del regolamento sulla cibersecurity nel 2019, e alla luce della rapida evoluzione del panorama delle minacce alla cibersecurity, è necessario rivedere il mandato dell'ENISA per stabilire una serie di compiti più mirati e rinnovati, al fine di sostenere in modo efficace ed efficiente gli sforzi degli Stati membri, delle istituzioni dell'UE e di altri portatori di interessi volti a garantire un ciberspazio sicuro nell'Unione europea. Attraverso il rafforzamento del quadro europeo di certificazione della cibersecurity, la proposta garantisce che l'UE disponga di un sistema di certificazione snello, moderno e adattabile che persegua le finalità delle azioni riguardanti le catene di approvvigionamento e la rapida attuazione del regolamento sulla cyberresilienza. In conclusione si delinea l'ambito del mandato proposto, rafforzando i settori in cui l'Agenzia ha dimostrato di apportare un chiaro valore aggiunto e introducendo nuovi settori in cui è necessario un sostegno in

⁸⁵ [Orientamenti politici 2024.](#)

⁸⁶ [Lettera d'incarico alla vicepresidente esecutiva Virkkunen.](#)

⁸⁷ [Relazione di Sauli Niinistö.](#)

⁸⁸ [Relazione Draghi sulla competitività dell'UE.](#)

⁸⁹ [Enrico Letta - *Much more than a market* \(aprile 2024\).](#)

considerazione delle nuove priorità e dei nuovi strumenti strategici e ai fini del rafforzamento del quadro europeo di certificazione della cibersicurezza.

La revisione del regolamento sulla cibersicurezza è pertanto destinata a costituire un importante cambio di passo per quanto riguarda la postura di cibersicurezza dell'UE e la sicurezza, la preparazione e la resilienza complessive dell'Unione europea.

- 1.5.2. *Valore aggiunto dell'intervento dell'UE (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini della presente sezione, per "valore aggiunto dell'intervento dell'UE" si intende il valore derivante dall'azione dell'Unione europea che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.*

Il regolamento sulla cibersicurezza è stato adottato nel 2019 sulla base giuridica dell'articolo 114 TFUE, che conferisce al legislatore dell'UE il potere di adottare misure di armonizzazione delle disposizioni legislative e regolamentari nazionali che hanno per oggetto l'instaurazione e il funzionamento del mercato interno.

La proposta di revisione del regolamento sulla cibersicurezza mira a razionalizzare la normativa in materia di cibersicurezza a livello dell'UE, integrando e rivedendo l'attuale regolamento sulla cibersicurezza, in vigore dal 2019. Gli obiettivi dell'attuale regolamento sulla cibersicurezza di conferire un mandato permanente all'Agenzia dell'Unione europea per la cibersicurezza, al fine di garantire un elevato livello comune di cibersicurezza in tutta l'UE e di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza, sono mantenuti nell'ambito della revisione avviata. Tali obiettivi, che sono già stati opportunamente esaminati nella proposta di regolamento sulla cibersicurezza del 2017, non possono essere conseguiti in misura sufficiente dagli Stati membri, ma possono esserlo solo a livello di Unione conformemente all'articolo 5 del trattato sull'Unione europea.

La proposta di revisione del regolamento sulla cibersicurezza pone chiaramente l'accento sulla razionalizzazione, sull'ordinamento secondo priorità e sulla codificazione dei compiti in tutte le normative in materia di cibersicurezza. Tali obiettivi potrebbero essere conseguiti solo a livello dell'UE e inoltre non esiste attualmente un'iniziativa di questo tipo. La nuova proposta rafforza ulteriormente la sicurezza delle catene di approvvigionamento e il settore della cibersicurezza all'interno dell'UE e migliora la preparazione e la resilienza degli Stati membri e dell'industria. Le dipendenze da soggetti stabiliti in paesi terzi che destano preoccupazioni per la cibersicurezza o controllati da soggetti di tali paesi terzi (fornitori ad alto rischio) interessano soggetti di tutta l'Unione, mentre gli incidenti di cibersicurezza significativi nelle catene di approvvigionamento spesso si diffondono oltre le frontiere nazionali. È improbabile che la questione possa essere affrontata in maniera efficiente solo con un intervento a livello nazionale.

I nuovi compiti assegnati all'ENISA sono di fondamentale importanza per conseguire livelli elevati di cibersicurezza in tutta l'UE. Sebbene l'Agenzia stia lavorando in coordinamento con altri organismi dell'UE che operano nel settore della sicurezza, come Europol e il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, che è responsabile dell'attuazione dei finanziamenti, la missione e i compiti dell'Agenzia sono unici e attualmente nessun altro organismo esercita questo tipo di responsabilità. Nell'ecosistema di

cibersicurezza dell'UE tutti i soggetti coinvolti operano in stretta sinergia e nell'ambito di mandati chiari. Pertanto la proposta relativa al regolamento sulla cibersicurezza 2 rafforza solo le parti in cui è evidente un chiaro valore aggiunto, garantendo che non vi siano ambiguità soprattutto in termini di duplicazione dei compiti, ma anche in termini di duplicazione dei finanziamenti, con altri organismi all'interno dell'ecosistema della cibersicurezza.

Ulteriori precisazioni

Il mandato dell'ENISA è stato ampliato mediante atti normativi successivi, senza una revisione globale delle relative responsabilità principali e risorse. Ciò ha determinato sovrapposizioni e inefficienze, nonché una definizione non adeguata delle priorità per quanto riguarda i compiti fondamentali a sostegno degli Stati membri.

Diversi Stati membri hanno attuato i propri sistemi nazionali di certificazione della cibersicurezza, che differiscono notevolmente in termini di ambito di applicazione e procedure di valutazione della conformità. Ciò determina una frammentazione del mercato e una duplicazione degli oneri a carico degli operatori e delle PMI, che mirano a ottenere la certificazione una sola volta e a operare in tutta l'UE. Il quadro europeo di certificazione della cibersicurezza è stato istituito dal regolamento sulla cibersicurezza con l'obiettivo di affrontare la frammentazione del mercato, ma l'attuazione è stata lenta e disomogenea.

Analogamente vari atti giuridici orizzontali e settoriali stabiliscono misure di cibersicurezza aventi finalità e obiettivi diversi, il che comporta anche differenze nei controlli di conformità e negli approcci di vigilanza definiti dagli Stati membri. Di conseguenza i soggetti, soprattutto le PMI o le imprese che operano in diversi Stati membri, devono sostenere oneri di conformità aggiuntivi, che incidono negativamente sulla loro competitività.

I diversi approcci alla sicurezza delle catene di approvvigionamento delle TIC e le diverse misure adottate dagli Stati membri determinano la frammentazione del mercato nonché requisiti di conformità divergenti per i soggetti. In particolare, data la natura transfrontaliera delle catene di approvvigionamento delle TIC, la frammentazione dei requisiti di conformità nel mercato interno comprometterebbe la certezza del diritto per i soggetti. L'esistenza di quadri nazionali divergenti per quanto riguarda l'applicazione di restrizioni per i fornitori ad alto rischio potrebbe creare ostacoli alla circolazione transfrontaliera di beni e servizi nel mercato interno. Infine, poiché le catene di approvvigionamento delle TIC possono coinvolgere soggetti e infrastrutture critici, indipendentemente dal luogo di stabilimento di tali fornitori, la frammentazione e le disparità nelle misure di cibersicurezza espongono tali soggetti a ulteriori rischi per la sicurezza.

Inoltre le proposte relative ai programmi del quadro finanziario pluriennale (QFP) comprendono una disposizione orizzontale che impone l'esclusione dei fornitori ad alto rischio individuati a norma del diritto dell'UE, al fine di tutelare l'integrità del bilancio dell'UE e garantire che la spesa dell'Unione non sia in contrasto con gli interessi essenziali dell'Unione in materia di sicurezza. Il quadro per le catene di approvvigionamento previsto dal regolamento sulla cibersicurezza sarebbe il meccanismo che consente tale individuazione nel settore delle catene di approvvigionamento delle TIC e può pertanto essere attuato solo a livello dell'UE.

Di regola gli attacchi informatici hanno carattere transfrontaliero, soprattutto se si considerano gli effetti di ricaduta che potrebbero derivare da un unico punto di

ingresso inizialmente interessato. Le minacce e i rischi per la cibersicurezza hanno un impatto sull'intera Unione europea e pertanto un quadro collettivo di conoscenza situazionale potrebbe migliorare in modo significativo i livelli di cibersicurezza dei soggetti all'interno dell'UE. Le proposte nell'ambito del mandato riveduto dell'ENISA affrontano tale questione con l'obiettivo di aumentare in misura significativa la ciberresilienza dell'UE.

In conclusione un intervento a livello dell'UE è cruciale in quanto le minacce alla cibersicurezza e le sfide correlate si estendono al di là dei singoli Stati membri. Soluzioni nazionali frammentate si sono rivelate insufficienti a garantire la fiducia e il coordinamento a livello di mercato. È necessario rivedere il quadro giuridico dell'UE per eliminare gli ostacoli, garantire un'attuazione coerente e sostenere gli Stati membri a fronte della crescente complessità del contesto normativo e del panorama delle minacce.

1.5.3. Insegnamenti tratti da esperienze analoghe

L'ENISA è stata istituita nel 2004 con un mandato a tempo determinato. Nel 2019 è entrato in vigore il regolamento sulla cibersicurezza, le cui disposizioni hanno conferito all'ENISA un mandato permanente affinché potesse realizzare l'obiettivo di diventare un centro di competenze informatiche in Europa. Oggi l'ENISA è un marchio riconosciuto e un partner affidabile per i portatori di interessi dell'UE. Le competenze dell'Agenzia sono state sviluppate gradualmente nel corso di 25 anni, rispecchiando l'evoluzione dell'ecosistema della cibersicurezza.

A norma dell'articolo 67 del regolamento sulla cibersicurezza, ogni cinque anni la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di apportare modifiche e le conseguenti implicazioni finanziarie. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni relative al quadro europeo di certificazione.

In conformità con le disposizioni del regolamento, la Commissione ha effettuato una valutazione dell'Agenzia e del quadro europeo di certificazione della cibersicurezza, che ha comportato una consultazione pubblica e uno studio indipendente. Conformemente alle pratiche per legiferare meglio, la Commissione ha inoltre avviato una consultazione pubblica riguardante specificamente la revisione del regolamento sulla cibersicurezza e ha pubblicato un invito a presentare contributi per raccogliere dati presso i gruppi di portatori di interessi. Nella valutazione si è giunti alla conclusione che l'ENISA ha assolto il suo mandato conseguendo quasi tutti i risultati previsti. Gli obiettivi dell'Agenzia sono tuttora pertinenti; in particolare i portatori di interessi hanno riconosciuto i risultati conseguiti in periodi di particolare difficoltà quali la pandemia di COVID-19 e la guerra di aggressione russa nei confronti dell'Ucraina. Nonostante i riscontri generalmente positivi dei portatori di interessi sui risultati conseguiti dall'ENISA, è anche emerso che esistono notevoli margini di miglioramento per soddisfare con continuità le loro aspettative.

Gli insegnamenti tratti hanno dimostrato che, per aumentare il livello di efficienza, sarebbe necessario imprimere all'ENISA un orientamento più strategico, definire le priorità per quanto riguarda i suoi compiti e rafforzare la sua capacità di fornire informazioni tempestive sulle minacce emergenti e strumenti strategici per affrontarle. Inoltre, come indicato da diversi portatori di interessi, l'ENISA potrebbe stabilire metodi più strutturati e trasparenti per dialogare con i soggetti privati, ponendo l'accento sul sostegno alle PMI. In tutte le consultazioni esterne è stata sottolineata l'importanza di aumentare i finanziamenti, il personale e la capacità

operativa dell'ENISA per consentirle di soddisfare le crescenti esigenze del panorama della cibersecurity dell'UE. Nella relazione di valutazione che ha fatto seguito allo studio i servizi della Commissione hanno constatato la chiara necessità di elaborare una normativa "a prova di futuro" che possa adattarsi alla complessità e alla rapida evoluzione del panorama delle minacce informatiche e di rafforzare l'Agenzia dotandola delle risorse necessarie affinché possa garantire il sostegno al conseguimento dei massimi livelli di cibersecurity in Europa. Sulla base dei dati raccolti e dell'esperienza acquisita nell'attuazione del regolamento sulla cibersecurity, si è giunti alla conclusione che il coordinamento con altri organismi dovrebbe essere semplificato e che occorre porre l'accento sul sostegno dell'ENISA all'attuazione del diritto dell'UE e sul sostegno fornito su richiesta alla Commissione per l'elaborazione della normativa in materia di cibersecurity. La proposta esamina le sinergie con le priorità geopolitiche della Commissione per affrontare rischi quali le crescenti dipendenze da soggetti stabiliti in paesi che destano preoccupazioni per la cibersecurity o controllati da tali paesi (fornitori ad alto rischio) in Europa. In quanto centro di competenze, attualmente l'ENISA detiene un patrimonio di informazioni fondamentali per creare una comprensione comune delle minacce e dei rischi a cui sono esposti i soggetti dell'UE. Il quadro proposto si basa pertanto sull'esperienza acquisita nell'applicazione dell'attuale regolamento sulla cibersecurity e promuove il coordinamento dei flussi di informazioni al fine di delineare un quadro globale di conoscenza situazionale.

Dalla valutazione del quadro europeo di certificazione della cibersecurity emergono diverse raccomandazioni strategiche. Sebbene l'ENISA svolga un ruolo cardine nel promuovere la cooperazione e la coesione operativa tra gli Stati membri e gli altri portatori di interessi, è emerso chiaramente che l'efficienza e l'efficacia del quadro europeo di certificazione della cibersecurity sono limitate soprattutto dalle complessità insite nei processi di adozione dei sistemi. Tali problemi hanno evidenziato la necessità di una revisione sostanziale delle strutture di governance per migliorare la chiarezza operativa e la responsabilità a tutti i livelli. La proposta di revisione del regolamento sulla cibersecurity risponde a tale necessità. L'esperienza acquisita con il funzionamento dell'attuale quadro europeo di certificazione della cibersecurity ha dimostrato la necessità di modernizzare e chiarire il quadro di certificazione e di introdurre una procedura di mantenimento per i sistemi di certificazione affinché tali sistemi possano rispondere alle esigenze del mercato e adeguarsi al panorama delle minacce. Infine il quadro originario non prevedeva rischi di natura non tecnica, che possono essere considerati una delle cause dello stallo nell'attuazione del quadro europeo di certificazione della cibersecurity nei sistemi 5G e cloud.

La complessità dell'ecosistema di cibersecurity dell'UE ha continuato ad aumentare in parallelo all'evoluzione delle minacce informatiche. Nelle osservazioni scritte dei portatori di interesse è emerso un forte consenso sulla necessità di ridurre gli oneri amministrativi, in particolare per le PMI, ed è stato chiesto di semplificare le procedure di conformità. Anche se la semplificazione sarà attuata soprattutto attraverso l'iniziativa "omnibus digitale", la proposta rispecchia le esigenze dei portatori di interessi introducendo modifiche della direttiva NIS 2 per agevolare il processo di attuazione.

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti rilevanti

Il regolamento sulla cibersicurezza 2 introduce le modifiche necessarie per dotare l'UE di strumenti e meccanismi che consentano di rispondere alle esigenze del panorama della cibersicurezza e di perseguire gli obiettivi strategici. Il regolamento proposto rafforzerà ulteriormente l'ENISA dotandola delle capacità necessarie per sostenere gli Stati membri nell'attuazione del diritto dell'UE e nel contrasto dei rischi informatici. Tenendo conto delle relazioni Draghi e Letta sopra citate, la proposta relativa al quadro finanziario pluriennale (QFP) per il periodo 2028-2034 è imperniata sulla competitività, sulla sicurezza e sull'autonomia strategica.

Di conseguenza le proposte nell'ambito del pacchetto di proposte orizzontali sul QFP per il periodo 2028-2034, in particolare quelle relative al Fondo europeo per la competitività e a Orizzonte Europa, introducono nuovi criteri di ammissibilità basati sul principio dell'esclusione dei "fornitori ad alto rischio" dai finanziamenti dell'UE. Il regolamento sulla cibersicurezza 2 è pienamente allineato a tale principio e inoltre rappresenta uno strumento che consente l'attuazione delle nuove prescrizioni relative ai "fornitori ad alto rischio", in quanto fornisce un quadro procedurale per la designazione dei paesi che destano preoccupazioni per la cibersicurezza a livello dell'UE. A tale riguardo, la proposta relativa al regolamento sulla cibersicurezza 2 è strategica ed è in linea con le priorità della Commissione per il conseguimento della sovranità tecnologica e il rafforzamento della competitività all'interno dell'Europa.

Il superamento della frammentazione esistente sarà affrontato attraverso una maggiore armonizzazione sul mercato della certificazione dell'UE, aumentando l'efficienza e la sostenibilità del processo di certificazione europeo.

Le proposte relative al QFP per il periodo 2028-2034 considerano prioritario lo sforzo di semplificazione nell'intero quadro. Le linee di bilancio passano da sette a quattro, mentre il numero dei programmi di finanziamento orizzontali è stato ridotto in modo significativo da 52 a 16, offrendo flessibilità e adattabilità alle esigenze attuali. La valutazione d'impatto per la revisione del regolamento sulla cibersicurezza ha sottolineato precisamente questi obiettivi: necessità di semplificare i requisiti di cibersicurezza nei diversi quadri legislativi, codificare i compiti dell'ENISA e concentrarli sui settori con il maggiore impatto per il conseguimento di una maggiore resilienza dell'ecosistema di cibersicurezza dell'UE. Sulla base di tali risultanze, le disposizioni proposte rafforzano la competitività attraverso la semplificazione, garantiscono livelli elevati di sicurezza attraverso un coordinamento rafforzato e l'analisi dei rischi e delle vulnerabilità e promuovono livelli più elevati di armonizzazione attraverso il superamento della frammentazione dovuta ai diversi sistemi nazionali. Inoltre l'ENISA è concepita per essere il principale motore delle iniziative di semplificazione digitale, in quanto integrerà il punto di accesso unico per le notifiche, come delineato nell'iniziativa "omnibus digitale"⁹⁰.

Una parte essenziale del pacchetto sul QFP per il periodo 2028-2034 è la proposta relativa a un nuovo fondo per la competitività, che riunisce oltre 16 programmi di finanziamento quali il programma Europa digitale, Health4EU, il Fondo europeo per la difesa ecc. Orizzonte Europa continuerà ad essere un programma a sé stante, strettamente collegato al Fondo europeo per la competitività. Questo nuovo quadro di

⁹⁰

Da aggiungere una volta pubblicata.

programmazione richiede un forte coordinamento e finanziamenti solidi che corrispondano alle priorità attuali. In tale prospettiva le disposizioni proposte nel regolamento sulla cibersicurezza 2 gettano le basi per approfondire il coordinamento tra l'ENISA e il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, responsabile dell'attuazione delle parti dei programmi Europa digitale e Orizzonte Europa relative alla cibersicurezza. Le disposizioni proposte garantiscono la coerenza e pongono l'accento sulle sinergie tra l'ENISA e il Centro. Lo stesso approccio è stato adottato ai fini della cooperazione con altre agenzie e organismi, come Europol.

Un altro aspetto dell'allineamento tra la proposta relativa al regolamento sulla cibersicurezza 2 e il QFP 2028-2034 è il principio di flessibilità. Con la revisione la Commissione propone un meccanismo di riscossione di "diritti" attraverso il quale l'ENISA potrà facilmente finanziare in parte le sue attività, più specificamente quelle connesse allo sviluppo e al mantenimento dei sistemi di attestazione delle competenze in materia di cibersicurezza, al trattamento delle domande di autorizzazione e alla concessione delle autorizzazioni ai fornitori, e al mantenimento dei sistemi europei di certificazione della cibersicurezza. Grazie a questa modifica, l'Agenzia potrà rispondere in modo flessibile e scalabile alle esigenze dei portatori di interessi e garantirà la sostenibilità della spesa attraverso il rifinanziamento dei suoi servizi.

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

Dall'ultima revisione del mandato dell'ENISA nel 2019 si osserva una tendenza verso una crescita esponenziale del contributo atteso dell'Agenzia a sostegno dell'attuazione del diritto dell'UE. Ciò ha determinato ogni anno richieste di rafforzamento del bilancio e di potenziamento del personale oltre i livelli inizialmente programmati. La revisione proposta introduce nuovi compiti importanti, oltre a integrare quelli previsti dal mandato dell'ENISA, che sono stati stabiliti da altri atti legislativi dopo l'adozione dell'attuale regolamento sulla cibersicurezza, ampliando in tal modo le capacità dell'ENISA, il che richiede ulteriori rinforzi in termini di risorse umane e finanziarie. Perseguendo l'obiettivo di far sì che la sicurezza digitale diventi il vantaggio competitivo dell'Europa, la proposta mira a produrre un impatto concreto all'interno dell'ecosistema della cibersicurezza. Ciò sarà possibile solo attraverso investimenti significativi che corrispondano all'effetto desiderato e soprattutto alle esigenze degli Stati membri e degli altri portatori di interessi. I nuovi compiti comportano la necessità di disporre di personale tecnico e specializzato, nonché investimenti finanziari (ad esempio per strumenti e piattaforme), il che potrebbe essere garantito solo attraverso una dotazione finanziaria supplementare a carico del bilancio dell'UE.

Con l'obiettivo di garantire una maggiore flessibilità e, nel contempo, un bilancio sostenibile a lungo termine per l'Agenzia, la revisione propone un meccanismo di riscossione di diritti che finanzia in parte i servizi forniti per il mantenimento del quadro di certificazione della cibersicurezza, nonché in relazione allo sviluppo e al mantenimento di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza e per il trattamento delle domande di autorizzazione e la concessione delle autorizzazioni ai fornitori.

Tutte le stime relative alle risorse aggiuntive previste nella revisione del regolamento sulla cibersicurezza sono effettuate tenendo presente il bilancio di base dell'ENISA

del 2025 (costi operativi e ETP). La Commissione ha effettuato un'analisi approfondita delle possibilità di riassegnazione in seno all'Agenzia per tenere conto dei nuovi compiti previsti dal mandato riveduto. Il fatto che l'Agenzia stia operando al massimo delle sue capacità senza alcuna possibilità di riduzione dei compiti e che il consiglio di amministrazione abbia già provveduto nel 2023 a un declassamento di priorità porta chiaramente a concludere che, nell'ambito della struttura attuale, non è possibile contemplare nuovi compiti senza un rafforzamento del bilancio e delle risorse umane. Inoltre molti dei compiti attuali sono coperti da accordi di contributo tra l'ENISA e la Commissione. La proposta mira pertanto ad aggiungere tali compiti al mandato dell'ENISA e a ottenere una dotazione di bilancio stabile per i prossimi anni.

Fatti salvi i negoziati relativi al prossimo QFP, gli stanziamenti assegnati all'Agenzia a decorrere dal 2028 saranno compensati mediante riassegnazioni da programmi nell'ambito del QFP 2028-2034. Qualora sia necessaria una riduzione compensativa, potrebbe essere necessario rivedere le risorse assegnate all'Agenzia nonché i flussi e le fonti di finanziamento corrispondenti. Le misure predisposte nel quadro della proposta relativa al regolamento sulla cibersicurezza 2 comportano anche l'assunzione di compiti aggiuntivi da parte della direzione generale partner dell'ENISA (ossia la direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie, DG CNECT). Va osservato in particolare che il quadro per le catene di approvvigionamento delle TIC sarà pienamente attuato a livello della Commissione, comprese l'analisi di mercato che accompagna le valutazioni dei rischi e la preparazione degli atti di esecuzione. La Commissione dovrà inoltre elaborare e adottare un'ulteriore serie di atti di esecuzione in relazione alle modalità dei meccanismi di riscossione di diritti. Sarà necessario prevedere una vigilanza e un'assistenza supplementari a livello della Commissione per l'applicazione del quadro europeo di certificazione della cibersicurezza, lo sviluppo di disposizioni tipo, il mantenimento dei sistemi di cibersicurezza, gli accordi di riconoscimento reciproco con i paesi terzi e l'attività di sorveglianza da parte dell'ENISA.

1.6. Durata della proposta/iniziativa e della relativa incidenza finanziaria

☐ **Durata limitata**

- ☐ in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA;
- ☐ incidenza finanziaria dal AAAA al AAAA per gli stanziamenti di impegno e dal AAAA al AAAA per gli stanziamenti di pagamento.

☒ **Durata illimitata**

- Attuazione con un periodo di avviamento dal AAAA al AAAA
- e successivo funzionamento a pieno ritmo.

1.7. Metodo o metodi di esecuzione del bilancio previsti

☐ **Gestione diretta** a opera della Commissione:

- ☐ a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione;
- ☐ a opera delle agenzie esecutive.

☐ **Gestione concorrente** con gli Stati membri.

☒ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

- ☐ a paesi terzi o organismi da questi designati;
- ☐ a organizzazioni internazionali e loro agenzie (specificare);
- ☐ alla Banca europea per gli investimenti e al Fondo europeo per gli investimenti;
- ☒ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;
- ☐ a organismi di diritto pubblico;
- ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico, nella misura in cui sono dotati di sufficienti garanzie finanziarie;
- ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;
- ☐ a organismi o persone incaricati di attuare azioni specifiche della politica estera e di sicurezza comune a norma del titolo V del trattato sull'Unione europea e indicati nel pertinente atto di base;
- ☐ a organismi di diritto privato di uno Stato membro o di diritto dell'Unione stabiliti in uno Stato membro e idonei ad essere incaricati, conformemente alla normativa settoriale, dell'esecuzione di fondi dell'Unione o delle garanzie di bilancio, nella misura in cui tali organismi sono controllati da organismi di diritto pubblico o da organismi di diritto privato investiti di attribuzioni di servizio pubblico e sono dotati di sufficienti garanzie finanziarie, sotto forma di responsabilità in solido da parte degli organismi di controllo o di garanzie finanziarie equivalenti, che possono essere limitate, per ciascuna azione, all'importo massimo del sostegno dell'Unione.

Osservazioni

--

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Le disposizioni in materia di monitoraggio e di relazioni seguiranno i principi delineati nel vigente regolamento sulla cibersicurezza⁹¹ e nel regolamento finanziario⁹², in linea con l'orientamento comune sulle agenzie decentrate⁹³.

A norma dell'articolo 40 del regolamento finanziario, ogni anno l'ENISA deve trasmettere alla Commissione, al Parlamento europeo e al Consiglio un documento unico di programmazione (DOCUP) contenente i programmi di lavoro annuali e pluriennali e la pianificazione delle risorse. Inoltre la proposta della Commissione di modifica del mandato dell'ENISA introduce l'obbligo per la Commissione, in qualità di membro del consiglio di amministrazione, di esprimere un voto favorevole ai fini dell'adozione del DOCUP da parte del consiglio di amministrazione dell'ENISA per le questioni relative alle risorse umane e al bilancio. La Commissione formulerà inoltre un parere sul progetto di DOCUP prima della procedura di votazione in seno al consiglio di amministrazione, al quale dovrà essere data attuazione prima dell'adozione del DOCUP⁹⁴.

L'ENISA deve presentare al consiglio di amministrazione una relazione annuale di attività consolidata che contenga in particolare informazioni sul conseguimento degli obiettivi e dei risultati stabiliti nel documento unico di programmazione. La relazione deve essere trasmessa anche alla Commissione, al Parlamento europeo e al Consiglio. Il direttore esecutivo dell'ENISA dovrebbe presentare al consiglio di amministrazione una valutazione ex post delle attività dell'ENISA ogni due anni. L'Agenzia dovrebbe inoltre elaborare un piano d'azione volto a dare seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti. Il consiglio di amministrazione dovrebbe avere il compito di controllare che sia dato adeguato seguito a tali conclusioni.

Presunti casi di cattiva amministrazione nelle attività dell'Agenzia possono formare oggetto di indagini da parte del Mediatore europeo ai sensi dell'articolo 228 del trattato.

Le fonti di dati per il previsto monitoraggio sarebbero prevalentemente l'ENISA, il gruppo europeo per la certificazione della cibersicurezza, il gruppo di cooperazione NIS, la rete di CSIRT e le autorità degli Stati membri. Oltre ai dati desunti dalle relazioni (comprese le relazioni annuali di attività) dell'ENISA, del gruppo europeo per la certificazione della cibersicurezza, del gruppo di cooperazione NIS, della rete di CSIRT e della Commissione, saranno utilizzati all'occorrenza specifici strumenti di raccolta dati (ad esempio indagini presso le autorità nazionali, Eurobarometro, studi specifici e relazioni redatte in esito alle esercitazioni paneuropee).

La proposta della Commissione relativa al regolamento sulla cibersicurezza 2 mantiene la prassi consolidata di riesame e di valutazione dell'Agenzia. Come indicato all'articolo 119 della proposta relativa al regolamento sulla cibersicurezza 2,

⁹¹ [Regolamento dell'UE sulla cibersicurezza | EUR-Lex](#)

⁹² [Financial regulation applicable to the general budget of the Union \(recast\) - Ufficio delle pubblicazioni dell'Unione europea.](#)

⁹³ https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.

⁹⁴ [Regolamento delegato \(UE\) 2019/715 - EN - EUR-Lex.](#)

la Commissione deve fare eseguire una valutazione dell'ENISA entro il [GG MM AAA] e successivamente ogni cinque anni. La valutazione riguarderà, in particolare, l'eventuale necessità di modificare il mandato dell'ENISA e le conseguenti implicazioni finanziarie. Una valutazione su due comprende un esame dei risultati conseguiti dall'ENISA, tenuto conto degli obiettivi, del mandato, della missione, della governance e dei compiti dell'Agenzia, anche per valutare se il mantenimento dell'ENISA sia ancora giustificato alla luce di tali obiettivi, mandato, missione, governance e compiti.

La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del regolamento per quanto riguarda gli obiettivi del quadro europeo di certificazione della cibersicurezza di garantire un livello adeguato di cibersicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e dei soggetti dell'Unione e di migliorare il funzionamento del mercato interno.

La valutazione esamina altresì l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo IV del presente regolamento per quanto riguarda gli obiettivi del quadro in materia di sicurezza delle catene di approvvigionamento delle TIC.

La Commissione riferisce al Parlamento europeo e al Consiglio su tutti i risultati e al consiglio di amministrazione sui risultati della valutazione per il titolo II del regolamento. I risultati della valutazione sono resi pubblici.

2.2. Sistema o sistemi di gestione e di controllo

2.2.1. Giustificazione del metodo o dei metodi di esecuzione del bilancio, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

Poiché la proposta incide sul contributo annuale dell'UE per l'ENISA, il bilancio dell'Unione sarà eseguito mediante gestione indiretta.

Conformemente al principio della sana gestione finanziaria, il bilancio dell'ENISA è eseguito secondo il principio del controllo interno efficace ed efficiente. L'ENISA è pertanto tenuta ad attuare un'adeguata strategia di controllo coordinata fra i pertinenti soggetti addetti alle varie fasi del controllo.

Per quanto riguarda i controlli ex post, l'ENISA, in quanto agenzia decentrata, è in particolare soggetta a:

- un audit interno da parte del servizio di audit interno della Commissione
- relazioni annuali da parte della Corte dei conti europea, contenenti una dichiarazione concernente l'affidabilità dei conti annuali e la legittimità e regolarità delle operazioni sottostanti
- discarico annuale concesso dal Parlamento europeo
- eventuali indagini dell'OLAF dirette ad accertare, in particolare, che le risorse stanziare alle agenzie siano usate correttamente.
- In quanto direzione generale partner dell'ENISA, la DG CNECT attuerà la sua strategia di controllo sulle agenzie decentrate per garantire una rendicontazione affidabile nel quadro della sua relazione annuale di attività (RAA). Mentre le agenzie decentrate hanno la piena responsabilità dell'esecuzione del proprio bilancio, la DG CNECT è responsabile del regolare pagamento dei contributi annuali stabiliti dall'autorità di bilancio.

- Il Mediatore europeo apporta infine un ulteriore livello di controllo e responsabilizzazione per l'ENISA.

Sulla base della valutazione dell'Agenzia e della valutazione d'impatto effettuata per presentare la proposta relativa al regolamento sulla cibersicurezza 2, è stato stabilito che è della massima importanza garantire risorse finanziarie adeguate affinché l'ENISA possa svolgere i compiti che le sono attribuiti nel quadro del nuovo mandato. Un'importante novità riguardante il mandato riveduto dell'Agenzia sarà l'introduzione di un meccanismo di riscossione di diritti, che è stato previsto per finanziare i costi di mantenimento dei sistemi europei di certificazione della cibersicurezza, adottati nell'ambito del quadro europeo di certificazione della cibersicurezza. Il quadro europeo di certificazione della cibersicurezza riveduto formalizzerà la procedura di mantenimento. L'attività di mantenimento sarà coordinata dall'ENISA e parzialmente finanziata tramite la riscossione di diritti, in modo da rispondere alle esigenze legate alla sua scalabilità (per mantenere un maggior numero di sistemi occorre disporre di personale aggiuntivo). L'Agenzia sarà inoltre dotata della capacità di fornire strumenti di prova per sostenere l'attuazione delle procedure di valutazione della conformità nell'ambito del quadro europeo di certificazione della cibersicurezza e di altre pertinenti normative dell'UE in materia di cibersicurezza. Le modalità relative ai diritti saranno stabilite in un atto di esecuzione adottato dalla Commissione. Inoltre la revisione prevede lo sviluppo e il mantenimento di sistemi europei di attestazione individuale e l'adozione di decisioni che autorizzino i fornitori a rilasciare attestati europei delle competenze individuali in materia di cibersicurezza.

2.2.2. *Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli*

La proposta relativa al regolamento sulla cibersicurezza 2 mira di per sé ad attenuare i rischi individuati nell'ambito del mandato dell'ENISA e del quadro europeo di certificazione della cibersicurezza, compresi il quadro in materia di sicurezza delle catene di approvvigionamento delle TIC e le disposizioni in materia di semplificazione. Più specificamente l'ENISA è un'agenzia dell'Unione europea già esistente e, nella revisione, si delinea ulteriormente il suo mandato, rafforzando i settori in cui l'Agenzia ha dimostrato di apportare un chiaro valore aggiunto e introducendo nuovi settori in cui è necessario un sostegno in considerazione delle nuove priorità e dei nuovi strumenti strategici, ad esempio la semplificazione attraverso l'integrazione di un punto di accesso unico per le comunicazioni, il sostegno per un quadro comune europeo di conoscenza situazionale e la cooperazione operativa, nonché il rafforzamento e la razionalizzazione del quadro europeo di certificazione della cibersicurezza.

Un altro rischio individuato e affrontato nella proposta deriva dal numero di accordi di contributo che la Commissione e l'Agenzia hanno concluso negli ultimi anni. A causa dell'attuale situazione geopolitica e della rapida evoluzione del panorama delle minacce alla cibersicurezza, a partire dal 2019 la Commissione ha concluso accordi di contributo con l'Agenzia per un valore totale di oltre 75 milioni di EUR. Considerando che i compiti attribuiti all'ENISA nell'ambito di tali accordi hanno ormai carattere permanente, l'instabilità del flusso di risorse di bilancio attraverso gli accordi di contributo presenta un rischio per il conseguimento a lungo termine dei risultati delle attività dell'ENISA.

Pertanto la proposta attuale prevede tra l'altro il rafforzamento della capacità dell'Agenzia in termini di risorse, con una ridefinizione dei suoi compiti e un conseguente incremento dell'efficienza. In particolare la possibilità di riscuotere diritti garantirà nel lungo periodo un circuito finanziario sostenibile in seno all'Agenzia grazie al rifinanziamento dei costi connessi al mantenimento dei sistemi europei di certificazione, adottati nell'ambito del quadro europeo di certificazione della cibersicurezza, alla verifica degli strumenti e allo sviluppo, al mantenimento e all'attuazione dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza. Si calcola che, nel lungo periodo, saranno realizzati risparmi per il bilancio dell'UE fino a 18,5 milioni di EUR all'anno. Sarà la Commissione a definire le modalità di riscossione e la composizione dei diritti attraverso l'adozione di atti di esecuzione.

L'aumento dei compiti operativi dell'Agenzia non rappresenta un rischio concreto. Tali compiti integrerebbero l'azione degli Stati membri e la sosterebbero, su richiesta. Saranno inoltre limitati a servizi predefiniti, per analogia con il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza)⁹⁵. I nuovi elementi/compiti previsti nella proposta apporteranno un valore aggiunto ai portatori di interessi europei, che trarranno vantaggio dal ruolo svolto dall'ENISA in quanto polo d'informazione che contribuisce alla condivisione delle informazioni e fornisce notifiche di allerta ai soggetti pertinenti.

Inoltre il modello proposto per l'Agenzia è in linea con l'orientamento comune della Commissione sulle agenzie decentrate, garantendo che vi sia un controllo sufficiente per garantire che l'ENISA persegua i suoi obiettivi. I rischi operativi e finanziari delle modifiche proposte sembrano essere limitati, in quanto le disposizioni sono elaborate in maniera tale da attenuare i rischi attuali. Tuttavia si possono prevedere alcuni aspetti negativi nel lungo periodo in relazione ai seguenti fattori:

- risorse operative messe a dura prova dalle crescenti esigenze operative degli Stati membri e dalla costante evoluzione delle minacce e dei rischi informatici nel settore della cibersicurezza;
- rapido aumento del bilancio, sommato alle aspettative di una rapida attuazione;
- mancanza di livelli adeguati di risorse finanziarie e umane per rispondere alle esigenze operative.

2.2.3. *Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto tra costi del controllo e valore dei fondi gestiti) e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)*

I costi sostenuti dalla DG CNECT per il monitoraggio e la vigilanza dei soggetti incaricati, compresa l'ENISA, ammontano a circa 5,25 milioni di EUR, come indicato nella relazione annuale di attività per il 2024⁹⁶. Tale importo comprende principalmente i costi per il personale e rappresenta lo 0,50 % dei pagamenti operativi effettuati a favore di tali soggetti nel corso del 2024. La percentuale totale dei costi del controllo è leggermente aumentata, passando dallo 0,46 % nel 2023 allo 0,50 % nel 2024, ma rimane relativamente stabile rispetto agli anni precedenti.

⁹⁵ <http://data.europa.eu/eli/reg/2019/881/oj>

⁹⁶ [CNECT_AAR_2024_final](#).

Più specificamente, per quanto riguarda l'ENISA, i costi del controllo nel 2024 ammontano a 0,32 milioni di EUR, pari allo 0,70 %, rispetto allo 0,69 % nel 2023 e all'1,22 % nel 2022. Dall'analisi emerge che i maggiori costi del controllo sono associati principalmente alla preparazione e al monitoraggio degli accordi di contributo tra la Commissione e l'Agenzia (principalmente costo delle risorse umane), che dovrebbero essere notevolmente ridotti nell'ambito del nuovo mandato; di conseguenza si prevedono livelli più elevati di efficienza. In termini di costi complessivi per la DG CNECT, rispetto agli altri soggetti incaricati l'ENISA si trova in posizione intermedia, a confronto con altri 11 soggetti.

La proposta relativa al regolamento sulla cibersicurezza 2 prevede un aumento del personale della DG CNECT con 50 ETP, di cui 1 ETP supplementare sarà specificamente assegnato ai compiti connessi alle attività svolte dalla DG CNECT in quanto direzione generale partner dell'Agenzia. La persona in questione avrà il compito di partecipare all'elaborazione del parere della Commissione sul documento unico di programmazione dell'ENISA e di monitorarne l'attuazione, contribuire a vigilare sull'elaborazione del bilancio dell'Agenzia e controllarne l'esecuzione, nonché coadiuvare l'Agenzia nello sviluppo delle sue attività conformemente alle politiche dell'Unione, anche partecipando alle riunioni pertinenti. L'azione è giustificata dai maggiori compiti di monitoraggio della DG CNECT, tra cui l'espressione di un voto favorevole da parte della Commissione su questioni relative al bilancio e alle risorse umane. Si osservi che l'attuazione delle disposizioni concernenti la designazione dei paesi che presentano rischi strategici per la cibersicurezza in relazione a specifici fornitori ad alto rischio di risorse chiave sarà un processo interamente guidato dalla Commissione. Il personale necessario per le valutazioni dei rischi in relazione a quanto sopra è stimato a 25 ETP. L'azione è giustificata dal volume di lavoro necessario per l'attuazione del quadro strategico, più specificamente per le seguenti attività: sostegno alle valutazioni coordinate dei rischi a livello dell'UE; analisi economica per ciascun prodotto/servizio TIC; preparazione dei rispettivi atti di esecuzione e monitoraggio dell'attuazione del quadro; esecuzione di valutazioni dell'assetto proprietario e di controllo. Si stima che il costo dei controlli a carico della Commissione per l'attuazione del quadro relativo alle catene di approvvigionamento risentirà in modo specifico del numero di valutazioni dell'assetto proprietario e di controllo che saranno effettuate dalla Commissione. I risultati di questo compito tuttavia contribuiranno notevolmente ai risparmi realizzati dagli Stati membri nelle attività di vigilanza dell'attuazione delle misure di attenuazione e degli obblighi imposti dal quadro ai soggetti rientranti nell'ambito di applicazione della direttiva NIS 2. Gli Stati membri saranno in grado di sfruttare direttamente i risultati delle valutazioni dell'assetto proprietario e di controllo, anziché spendere singolarmente risorse per soddisfare le stesse esigenze di valutazione. Per il rafforzamento del quadro europeo di certificazione della cibersicurezza, l'attività di normazione e l'esecuzione delle attività correlate, nonché per l'attuazione della direttiva NIS 2 (ad esempio per le rispettive necessità di attuazione, gli atti di esecuzione per l'imposizione di diritti e il sostegno al mantenimento dei sistemi di certificazione e dei sistemi di attestazione delle competenze) il fabbisogno di risorse umane è stato stimato a 19 ETP, mentre per le politiche in materia di cooperazione operativa e di conoscenza situazionale sono necessari altri 5 ETP. Per la descrizione completa dei compiti, cfr. sezione 3.2.4.

Nella sua relazione annuale di attività consolidata per il 2023⁹⁷, l'ENISA ha valutato positivamente i propri sistemi di controllo interno e ha fornito una dichiarazione di affidabilità senza rilievi. Nella sua relazione annuale sulle agenzie dell'UE per l'esercizio finanziario 2023, la Corte dei conti europea ha espresso un giudizio di audit positivo sui conti e un giudizio con rilievi sulla legittimità e regolarità dei pagamenti alla base dei conti (cfr. anche punto 2.2.2). La DG CNECT ha preso atto della relazione ma ha concluso che essa non incide sull'efficacia della vigilanza da parte della DG CNECT. L'ENISA inoltre riferisce periodicamente sulle misure adottate per evitare il ripetersi delle constatazioni e, per il momento, non vi sono elementi che indichino che il tasso di errore sia destinato a peggiorare/sarà superiore al 2 % nei prossimi anni.

L'articolo 80, paragrafo 2, del regolamento finanziario dell'ENISA⁹⁸ prevede inoltre la possibilità per l'Agenzia di condividere una struttura di audit interno con altri organismi dell'Unione che operano nello stesso settore se la struttura di audit interno di un solo organismo dell'Unione non è efficiente in termini di costi.

In conclusione, considerando la proposta di aumentare le dimensioni dell'Agenzia di oltre il 100 % a fronte di un incremento relativamente contenuto dei costi del controllo, l'analisi rivela un rapporto costo/efficacia soddisfacente. Alla luce di tutti i dati disponibili, non vi sono elementi indicanti che l'errore previsto possa essere superiore al 2 %.

2.3. Misure di prevenzione delle frodi e delle irregolarità

L'Agenzia dell'Unione europea per la cibersicurezza applicherà le norme più rigorose in materia di prevenzione delle frodi e delle irregolarità.

Il controllo dei pagamenti per tutti i servizi o gli studi necessari è effettuato dal personale dell'Agenzia prima del pagamento stesso, tenendo conto degli obblighi contrattuali, dei principi economici e delle prassi finanziarie o di sana gestione. Disposizioni antifrode (vigilanza, obblighi di comunicazione, ecc.) saranno inserite in tutti gli accordi e i contratti stipulati tra l'Agenzia e i beneficiari dei pagamenti.

Ai fini della lotta contro la frode, la corruzione e altre attività illecite si applicano senza limitazioni le disposizioni del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro	Linea di bilancio	Natura della spesa	Partecipazione
--------------------	-------------------	--------------------	----------------

⁹⁷ [enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf](https://enisa.europa.eu/sites/default/files/2024-11/2023_Consolidated_Annual_Activity_Report_1.pdf).
⁹⁸ [MB Decision 2019_8 Financial rules_adopted.pdf](#).

finanziario pluriennale	Numero	Diss./Non diss. ⁹⁹	di paesi EFTA ¹⁰⁰	di paesi candidati e potenziali candidati ¹⁰¹	di altri paesi terzi	altre entrate con destinazione specifica
	[XX.YY.YY.YY]	Non diss.	SÌ	NO	NO	SÌ/NO
	[XX.YY.YY.YY]	Diss./No n diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO
	[XX.YY.YY.YY]	Diss./No n diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

- Nuove linee di bilancio di cui è chiesta la creazione

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati e potenziali candidati	di altri paesi terzi	altre entrate con destinazione specifica
	[XX.YY.YY.YY]	Diss./No n diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO
	[XX.YY.YY.YY]	Diss./No n diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO
	[XX.YY.YY.YY]	Diss./No n diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

⁹⁹ Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

¹⁰⁰ EFTA: Associazione europea di libero scambio.

¹⁰¹ Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

- ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.
- ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito.

3.2.1.1. Stanziamenti dal bilancio votato

Mio EUR (al terzo decimale)

Agenzia: ENISA	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTALE QFP 2028- 2034
Linea di bilancio: <.....> / Contributo aggiuntivo del bilancio dell'UE all'agenzia	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006

Gli stanziamenti / Il contributo del bilancio dell'UE all'agenzia saranno compensati / sarà compensato da una riduzione della dotazione del seguente programma <.....> / della seguente linea di bilancio: <.....> / nell'anno / negli anni: <.....>.

			Anno	Anno	Anno	Anno	Anno	Anno	Anno	TOTALE QFP 2028-2034	
			2028	2029	2030	2031	2032	2033	2034		
TOTALE stanziamenti operativi	Impegni	4)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006	
	Pagamenti	5)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006	
TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici		6)	1,365	1,365	1,470	1,785	2,100	2,415	2,625	13,125	
TOTALE stanziamenti	Impegni		=4+6	22,265	21,959	26,808	28,586	28,901	28,716	28,926	186,161

per la RUBRICA 2 del quadro finanziario pluriennale										
	Pagamenti	=5+6	22,265	20,890	24,851	26,254	26,254	25,754	25,754	186,161
DG: CNECT			Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTALE QFP 2028- 2034
• Risorse umane			3,693	3,693	4,574	5,277	5,980	6,683	7,475	37,375
• Altre spese amministrative			0	0	0	0	0	0	0	0
TOTALE DG CNECT	Stanziamenti	3,693	3,693	4,574	5,277	5,980	6,683	7,475	37,375	

TOTALE stanziamenti per la RUBRICA 4 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	2,328	2,328	3,104	3,492	3,880	4,268	4,850	24,25
--	--	-------	-------	-------	-------	-------	-------	-------	-------

Mio EUR (al terzo decimale)

	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTALE QFP 2028-2034
--	--------------	--------------	--------------	--------------	--------------	--------------	--------------	-------------------------

TOTALE stanziamenti per le RUBRICHE da 1 a 4	Impegni	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38
del quadro finanziario pluriennale	Pagamenti	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi (da non compilarsi per le agenzie decentrate)

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ↓			Anno 2028		Anno 2029		Anno 2030		Anno 2031		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. sezione 1.6)						TOTALE	
	RISULTATI																	
	Tipo ¹⁰²	Costo medio	z:	Costo	z:	Costo	z:	Costo	z:	Costo	z:	Costo	z:	Costo	z:	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1 ¹⁰³ ...																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		

¹⁰² I risultati sono i prodotti e i servizi da fornire (ad es. numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

¹⁰³ Come descritto nella sezione 1.3.2. "Obiettivi specifici".

- Risultato																		
Totale parziale obiettivo specifico 2																		
TOTALE																		

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

- ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.
- ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito.

3.2.3.1. Stanziamenti dal bilancio votato

(aggiuntivo)

STANZIAMENTI VOTATI	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTALE 2028-2034
RUBRICA 4								
Risorse umane	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Altre spese amministrative	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Totale parziale RUBRICA 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Esclusa la RUBRICA 4								
Risorse umane	1,365	1,365	1,470	1,785	2,100	2,415	2,625	13,125
Altre spese amministrative	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Totale parziale esclusa la RUBRICA 4	1,365	1,365	1,470	1,785	2,100	2,415	2,625	13,125
TOTALE	3,693	3,693	4,574	5,277	5,980	6,683	7,475	37,375

3.2.4. Fabbisogno previsto di risorse umane (aggiuntivo)

- ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.
- ☒ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito.

3.2.4.1. Finanziamento a titolo del bilancio votato

Stima da esprimere in equivalenti a tempo pieno (ETP)¹⁰⁴

STANZIAMENTI VOTATI	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034
• Posti della tabella dell'organico (funzionari e agenti temporanei)							
20 01 02 01 (sede e uffici di rappresentanza della Commissione)	12	12	16	18	20	22	25
20 01 02 03 (delegazioni UE)	0	0	0	0	0	0	0
(ricerca indiretta)	0	0	0	0	0	0	0
(ricerca diretta)	0	0	0	0	0	0	0
Altre linee di bilancio (specificare)	0	0	0	0	0	0	0
• Personale esterno (in ETP)							
20 02 01 (AC, END della dotazione globale)	0	0	0	0	0	0	0

¹⁰⁴ Specificare sotto alla tabella quanti ETP nel numero indicato sono già assegnati alla gestione dell'azione e/o possono essere riassegnati all'interno della DG e qual è il fabbisogno netto.

20 02 03 (AC, AL, END e JPD nelle delegazioni UE)		0	0	0	0	0	0	0
Linea di sostegno amministrativo [XX.01.YY.YY]	- in sede	0	0	0	0	0	0	0
	- nelle delegazioni UE	0	0	0	0	0	0	0
(AC, END - ricerca indiretta)		0	0	0	0	0	0	0
(AC, END - ricerca diretta)		0	0	0	0	0	0	0
Altre linee di bilancio (specificare) - rubrica 4		0	0	0	0	0	0	0
Altre linee di bilancio (specificare) - esclusa la rubrica 4		13	13	14	17	20	23	25
TOTALE		25	25	30	35	40	45	50

Personale necessario per l'attuazione della proposta (in ETP):

	Da coprire con il personale attualmente disponibile presso i servizi della Commissione	Personale supplementare eccezionale		
		Da finanziare a titolo della rubrica 7 o della ricerca	Da finanziare a titolo della linea BA	Da finanziare mediante diritti
Posti della tabella dell'organico		25		
Personale esterno (AC, END, INT)			25	

L'impatto stimato sulle spese e sul personale per il 2028 e gli anni successivi è indicativo e non pregiudica il prossimo quadro finanziario pluriennale. La fonte di finanziamento e la portata dell'impegno finanziario dell'Unione nel periodo successivo al 2027 restano subordinate all'esito dei negoziati interistituzionali sul QFP 2028-2034, alla procedura di bilancio annuale e al meccanismo di orientamento.

Descrizione dei compiti che la DG di settore deve svolgere in seno alla Commissione

Funzionari e agenti temporanei	Coordinamento dell'ENISA (1) Rappresentare la Commissione nel consiglio di amministrazione dell'Agenzia. Redigere il parere della Commissione sul documento unico di programmazione dell'ENISA e controllarne l'applicazione. Vigilare sull'elaborazione del bilancio dell'Agenzia e controllarne l'esecuzione. Coadiuvare l'Agenzia nello sviluppo delle sue attività conformemente alle politiche dell'Unione, anche partecipando alle riunioni pertinenti. Sistemi di attestazione delle competenze / Accademia per le competenze (2) Sarà necessario prevedere personale supplementare presso la DG CNECT per la preparazione degli atti di esecuzione che stabiliscono i diritti che l'ENISA riscuoterà presso i richiedenti che presentano domanda per diventare fornitori autorizzati. Tali atti di esecuzione saranno almeno 12, uno per ciascun profilo dell'ECSF. Catena di approvvigionamento (25) Sostenere la preparazione delle valutazioni coordinate dei rischi a livello dell'Unione. Effettuare un'analisi economica per ciascun prodotto o servizio TIC considerato. Redigere i rispettivi atti di esecuzione per l'individuazione delle risorse chiave, le misure di attenuazione proposte e la designazione dei paesi che presentano rischi strategici per la cibersicurezza in relazione a specifiche risorse chiave, l'individuazione dei fornitori ad alto rischio, la verifica delle richieste di esenzione e la preparazione delle decisioni della Commissione. Sostenere l'attuazione e la vigilanza delle misure adottate. Quadro europeo di certificazione della cibersicurezza, normazione ed esecuzione delle attività correlate, attuazione della direttiva NIS 2 (17) Applicazione del regolamento sulla cibersicurezza, in particolare per quanto riguarda la governance degli organismi di valutazione della conformità (contestazione della competenza) Coinvolgimento dei portatori di interessi (e assemblea) Riconoscimento reciproco con i paesi terzi Elaborazione di atti di esecuzione standardizzati (richieste dettagliate soggette a consultazioni ed elaborazione di disposizioni tipo) Mantenimento dei sistemi, riesame giuridico, procedura di comitato Coordinamento con il gruppo di cooperazione NIS e mantenimento dei sistemi dei soggetti Atti di esecuzione ai sensi della direttiva NIS 2 Allineamento degli organismi di valutazione della conformità al regolamento sulla cibersicurezza, presunzione di conformità + normazione Coordinamento tra le autorità di vigilanza del mercato e le autorità nazionali di certificazione della cibersicurezza Allineamento tecnico tra il regolamento sulla ciberresilienza e i sistemi di certificazione Coordinamento operativo e conoscenza situazionale (5) Competenze settoriali e relative agli autori delle minacce per contribuire alla conoscenza situazionale, a livello dell'UE, delle minacce alle infrastrutture critiche, anche attraverso tecnologie emergenti Coordinamento con l'ENISA e altri soggetti e reti dell'UE per prepararsi agli incidenti informatici significativi e su vasta scala
---------------------------------------	---

Personale esterno	Come sopra
-------------------	------------

Descrizione dei compiti aggiuntivi che devono essere svolti dall'ENISA:

Funzionari e agenti temporanei	Gestione della riserva dell'UE per la cibersicurezza (gestori nazionali e sostegno all'attuazione, mentre i costi operativi effettivi della riserva sono coperti come previsto dal regolamento sulla ciber-solidarietà) (10) Gestione della piattaforma unica di segnalazione ai sensi del regolamento sulla ciberresilienza (funzionamento) (9) Servizi di gestione delle vulnerabilità connessi alla piattaforma unica di segnalazione (4) Ampliamento della piattaforma unica di segnalazione con integrazione del punto di accesso unico (sviluppo e gestione) (8) Elaborazione di orientamenti tecnici, competenze in materia di sicurezza dei prodotti e analisi di mercato a sostegno dell'attuazione del regolamento sulla ciberresilienza (7) Attività di normazione a sostegno dell'attuazione del regolamento sulla ciberresilienza / certificazione / NIS 2 (4) Sostegno alle attività di vigilanza del mercato nell'ambito del regolamento sulla ciberresilienza (4) Sostegno per le prove di conformità e le valutazioni della sicurezza dei prodotti (4) Sostegno agli Stati membri nell'assistenza reciproca (3) Fornitura di servizi di gestione delle vulnerabilità, mantenimento della banca dati europea delle vulnerabilità ed espletamento delle funzioni di consulenza e arricchimento (divulgazione coordinata delle vulnerabilità) (15) Cooperazione operativa e conoscenza situazionale - piattaforme per l'attenuazione e il sostegno quali CNW/CyCLONE; sostegno allo svolgimento dei compiti relativi alle notifiche di allerta; sostegno al coordinamento rafforzato con altri soggetti pertinenti al fine di sviluppare archivi di intelligence verificata e affidabile sulle minacce informatiche (articolo 11, paragrafo 1 bis, del regolamento sulla cibersicurezza 2) (5) Sostegno alla resilienza dei settori critici (compresa l'attuazione del piano d'azione per la cibersicurezza nel settore sanitario) (4) Sviluppo di sistemi di attestazione delle competenze (2) Mantenimento e sorveglianza dei sistemi di attestazione delle competenze (6) Amministrazione (contabile per la riscossione dei diritti/risorse umane/informatica) (8) Mantenimento dei sistemi di certificazione (11) Compiti orizzontali - maggiore coinvolgimento dei portatori di interessi, elaborazione di specifiche tecniche e partecipazione alle attività di normazione a sostegno dei sistemi (1)
Personale esterno	Come sopra Obbligo di due END per Stato membro che coadiuveranno l'Agenzia nelle sue attività e fungeranno da funzionari nazionali di collegamento, con particolare attenzione alla cooperazione operativa e alla divulgazione coordinata delle vulnerabilità. 13) Per quanto riguarda gli altri 27 END non si prevedono costi e dunque non vi è alcuna incidenza sul bilancio.

Costi operativi aggiuntivi all'anno per l'ENISA nel periodo 2028-2034:

Costo	Bilancio	Calendario	Spiegazione
Sito web sulle competenze in materia di cibersicurezza	750 000 EUR	50 % nel 2029 50 % nel 2030	Per garantire la trasparenza delle procedure, la proposta impone all'ENISA di gestire un sito web che riporti i profili dell'ECFS, i sistemi di attestazione, informazioni sui diritti riscossi per ciascun sistema, l'importo dei diritti raccomandati per ciascun attestato e l'elenco dei fornitori autorizzati di attestati.
Divulgazione coordinata delle vulnerabilità	1 milione di EUR	A decorrere dal 2028	La sicurezza dei prodotti e dei servizi utilizzati nelle infrastrutture critiche dell'UE dipende in larga misura dalla condivisione tempestiva di informazioni sulle vulnerabilità rilevate e sul modo in cui è possibile

			attenuarle.
Intelligence sulle minacce alla cibersicurezza	3 milioni di EUR	A decorrere dal 2028	Creare un quadro di conoscenza situazionale attraverso la cooperazione tra l'ENISA e la Commissione.
Punto di accesso unico	8 milioni di EUR	6 milioni di EUR nel 2028 500 000 EUR nel 2029 500 000 EUR nel 2030 500 000 EUR nel 2031 500 000 EUR nel 2032	Essere in grado di conseguire gli obiettivi della proposta "omnibus digitale" della Commissione per semplificare il rispetto degli obblighi di segnalazione degli incidenti di cibersicurezza e delle violazioni dei dati sviluppando e mantenendo un punto di accesso unico.
Manutenzione della piattaforma unica di segnalazione istituita dal regolamento sulla ciberresilienza e altre attività	3 milioni di EUR	A decorrere dal 2028	La piattaforma unica di segnalazione introdotta dai legislatori costituisce il più grande sistema informatico mai sviluppato nella storia dell'ENISA nonché un pilastro fondamentale del regolamento sulla

			ciberresilienza. La sua creazione è attualmente finanziata mediante un accordo di contributo, ma la sua gestione quotidiana richiederà ETP (cfr. sopra) e comporterà costi operativi. L'ENISA ha un ruolo fondamentale da svolgere per garantire il successo del quadro dell'Unione in materia di sicurezza dei prodotti (regolamento sulla ciberresilienza).
Maturità dell'ENISA in materia di sicurezza delle comunicazioni e di cibersecurity	più di 2 milioni di EUR	1,1 milioni di EUR di investimenti nel 2028 (piattaforme CyCLONE/CSIRT + sicurezza delle comunicazioni) 1 milione di EUR all'anno per la manutenzione a decorrere dal 2029 1,5 milioni di EUR per la maturità in materia di cibersecurity	Garantire la cibersecurity dell'Agenzia e degli strumenti di comunicazione.
Mantenimento della certificazione della	1 400 000 milioni di EUR	600 000 EUR nel 2028 1 000 000 di EUR	Coperto dai diritti riscossi (integralmente a partire dal

cibersicurezza		nel 2029 1 200 000 EUR nel 2030 1 400 000 EUR nel 2031 1 400 000 EUR nel 2032 1 400 000 EUR nel 2033 1 400 000 EUR nel 2034	2032)
Sistemi di attestazione della cibersicurezza	212 920 EUR	Dal 2030 coperto al 50 % dal bilancio UE	Dal 2033 interamente coperto dai diritti riscossi

3.2.5. *Panoramica dell'incidenza prevista sugli investimenti connessi a tecnologie digitali*

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 4 should be presented in the designated line.

The appropriations under Headings 1-3 should be reflected as “Policy IT expenditure on operational programmes”. This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 “Digital dimensions”.

TOTALE stanziamenti per fini digitali e informatici	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTALE QFP 2028-2034
RUBRICA 4								
Spese informatiche (istituzionali)	0	0	0	0	0	0	0	0
Totale parziale RUBRICA 4	0	0	0	0	0	0	0	0
Esclusa la RUBRICA 4								

Spese informatiche per la politica per i programmi operativi	0	0	0	0	0	0	0	0
Totale parziale esclusa la RUBRICA 4	0	0	0	0	0	0	0	0
TOTALE	0	0	0	0	0	0	0	0

3.2.6. Compatibilità con il quadro finanziario pluriennale attuale

La proposta/iniziativa:

- ☒ può essere interamente finanziata mediante riassegnazione all'interno della pertinente rubrica del quadro finanziario pluriennale (QFP).

Fatti salvi i negoziati relativi al prossimo QFP, gli stanziamenti assegnati all'Agenzia a decorrere dal 2028 saranno compensati mediante riassegnazioni da programmi nell'ambito del QFP 2028-2034. Qualora sia necessaria una riduzione compensativa, potrebbe essere necessario rivedere le risorse assegnate all'Agenzia nonché i flussi e le fonti di finanziamento corrispondenti.

- ☐ comporta l'uso del margine non assegnato della pertinente rubrica del QFP e/o l'uso degli strumenti speciali definiti nel regolamento QFP.
- ☐ comporta una revisione del QFP.

3.2.7. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

- ☒ non prevede cofinanziamenti da parte di terzi.
- ☐ prevede il cofinanziamento da parte di terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Totale
Specificare l'organismo di cofinanziamento					
TOTALE stanziamenti cofinanziati					

3.2.8. Stima del fabbisogno di risorse umane e dell'utilizzo degli stanziamenti necessari in un'agenzia decentrata

Fabbisogno di personale supplementare (in equivalenti a tempo pieno)

Agenzia: ENISA	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034
Agenti temporanei (gradi AD)	5	11	17	19	19	19	19

Agenti temporanei (gradi AST)	4	7	11	12	12	12	12
Totale parziale agenti temporanei (AD+AST)	9	18	28	31	31	31	31
Agenti contrattuali	22	44	66	74	74	74	74
Esperti nazionali distaccati	4	8	11	13	13	13	13
Totale parziale agenti contrattuali ed esperti nazionali distaccati	26	52	77	87	87	87	87
TOTALE personale	35	70	105	118	118	118	118

Stanziamenti coperti dal contributo del bilancio dell'UE in Mio EUR (al terzo decimale)

Agenzia: ENISA	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTAL E 2028-2034
Titolo 1: spese per il personale	4,488	8,466	12,507	13,648	10,584	10,012	9,537	87,766
Titolo 2: spese per infrastrutture e funzionamento								
Titolo 3: spese operative	16,413	11,588	11,528	11,788	11,613	11,613	11,113	85,240
TOTALE stanziamenti coperti dal bilancio dell'UE	20,901	20,054	24,035	25,437	22,197	21,625	21,151	155,4

Stanziamenti coperti dai diritti, se del caso, in Mio EUR (al terzo decimale)

Agenzia: ENISA	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTAL E 2028-2034
Titolo 1: spese per il personale		0,510	1,043	1,539	4,604	5,176	5,650	18,522
Titolo 2: spese per infrastrutture e funzionamento								0,000
Titolo 3: spese operative								0,000
TOTALE stanziamenti coperti dai diritti	0,000	0,510	1,043	1,539	4,604	5,176	5,650	18,522

Panoramica/sintesi del fabbisogno di risorse umane e di stanziamenti (in Mio EUR) in base alla proposta / all'iniziativa in un'agenzia decentrata

Agenzia: ENISA	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034	TOTAL E 2028-2034
----------------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	-------------------

Agenti temporanei (AD+AST)	9	18	28	31	31	31	31	31
Agenti contrattuali	22	44	66	74	74	74	74	74
Esperti nazionali distaccati	4	8	11	13	13	13	13	13
Totale personale	35	70	105	118	118	118	118	118
Stanziamanti coperti dal bilancio dell'UE	20,901	20,054	24,035	25,437	22,197	21,625	21,151	155,4
Stanziamanti coperti dai diritti (se del caso)	0,000	0,510	1,043	1,539	4,604	5,176	5,650	18,522
Stanziamanti cofinanziati (se del caso)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
TOTALE stanziamenti	20,901	20,564	25,078	26,976	26,801	26,801	26,801	173,922

3.3. Incidenza prevista sulle entrate

- ☒ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.
- ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:
 - ☐ sulle risorse proprie.
 - ☐ su altre entrate.
 - ☐ indicare se le entrate sono destinate a linee di spesa specifiche.

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamanti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa ¹⁰⁵						
		Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033	Anno 2034
Articolo								

Per quanto riguarda le entrate con destinazione specifica, precisare la linea o le linee di spesa interessate.

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni)

I meccanismi di riscossione di diritti riguardano tre settori di attività dell'ENISA:

¹⁰⁵ Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.

- Diritti in relazione all'autorizzazione dei fornitori nell'ambito dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza.

I diritti riscossi in relazione a tale attività saranno definiti in un atto di esecuzione, a seguito dell'adozione del regolamento sulla cibersicurezza riveduto. Tuttavia, per poter stimare gli investimenti necessari e i costi, i calcoli sono stati effettuati utilizzando un modello esistente in uno Stato membro dell'UE¹⁰⁶. Il modello prevede un pagamento una tantum e un diritto annuale.

Costi fissi: 8 540 EUR

Diritto annuale: 800 EUR

I diritti sono destinati a rifinanziare i costi per questa specifica attività. I costi sono stati stimati a 1 064 600 EUR su un periodo di cinque anni. Tale importo comprende i costi specifici delle attività che sono connessi allo sviluppo e al mantenimento dei sistemi, comprese le spese dei membri di un gruppo di lavoro ad hoc incaricato di assistere l'ENISA nello sviluppo dei sistemi (rimborso delle spese e pagamento dei relatori), le missioni di audit in loco presso i fornitori e la formazione dei valutatori per garantire un'applicazione omogenea dei sistemi:

A) spese del gruppo di lavoro ad hoc: 800 000 EUR

B) formazione di due valutatori per Stato membro: 129 600 EUR

C) audit di un soggetto per Stato membro: 135 000 EUR

$(A + B + C) / 5 = 212\,920$ EUR (costi annui)

La proposta ha previsto un periodo di transizione e un investimento iniziale nei primi tre anni. Durante il periodo di transizione i costi saranno coperti dal bilancio dell'UE; nel quarto e nel quinto anno la copertura sarà del 50 %, mentre nel sesto e nel settimo anno è prevista la piena applicazione dei diritti.

Anno	Diritti
2028	0
2029	0
2030	0
2031	106 460 (entrate)
2032	106 460 (entrate)
2033	212 920 (entrate)
2034	212 920 (entrate)

- Diritti relativi alla copertura dei costi di mantenimento di un sistema di certificazione della cibersicurezza adottato nell'ambito del quadro europeo di certificazione della cibersicurezza.

¹⁰⁶

Decision RR-02: Price list of SNAS services: <https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf>,

I diritti riscossi in relazione a tale attività saranno definiti in un atto di esecuzione, a seguito dell'adozione del regolamento sulla cibersicurezza riveduto. Le stime dei costi di mantenimento di un sistema si basano su un'analisi di mercato, inclusa nella valutazione d'impatto della proposta di revisione del regolamento sulla cibersicurezza. I costi totali dell'attività per un periodo di cinque anni sono stimati a 5 600 000 EUR per quanto riguarda i costi operativi e a 7 100 000 EUR per gli ETP.

Il costo annuo delle attività di mantenimento è stimato, sulla base dell'esperienza attuale, a 200 000 EUR per anno di mantenimento del sistema¹⁰⁷ e si prevedono due ETP per tali attività (con un costo annuo di 125 887 EUR per ETP), tenendo conto dell'anno di prevista adozione di tali sistemi. Si prevede che le entrate derivanti dalla riscossione di tali diritti aumenteranno progressivamente con l'adozione di ogni nuovo sistema e con la graduale adesione a tali sistemi. Finora è stato adottato un solo sistema (EUCC) nell'ambito del quadro europeo di certificazione della cibersicurezza e le prime entrate derivanti dal mantenimento di tale sistema sono previste per il 2029. Si prevede che i costi saranno coperti entro il 2032.

Le entrate stimate sono state calcolate sulla base di ipotesi specifiche per ciascun sistema potenziale in relazione ai seguenti aspetti: la diffusione prevista (numero di certificati da rilasciare), la durata di validità di ciascun certificato e il numero di organismi di valutazione della conformità attivi. Si prevedono notevoli entrate derivanti dall'adesione a un futuro sistema di certificazione della postura di cibersicurezza.

Anno	Entrate (percentuale dei costi coperti/pagati dal bilancio dell'UE)
2028	0
2029	250 000 (11 %/ - 1 350 000 EUR) – un solo sistema (EUCC)
2030	783 000 (29 %/ - 2 000 000 EUR) – tre sistemi (EUCC, portafoglio digitale, servizi di sicurezza gestiti)
2031	783 000 (25 %/ - 1 930 000 EUR) – tre sistemi (EUCC, portafoglio digitale, servizi di sicurezza gestiti)
2032	3 850 000 (122 %/ - 2 400 000 EUR) – cinque sistemi (EUCC, portafoglio digitale, servizi di sicurezza gestiti, EUCS, 5G)
2033	4 000 000 (126 %/ + 685 000 EUR) – sei sistemi (EUCC, portafoglio digitale, servizi di sicurezza gestiti, EUCS, 5G, postura di cibersicurezza)
2034	4 500 000 (141 %/ + 825 000 EUR) – sette sistemi
Diritti relativi agli strumenti di prova a sostegno delle procedure di valutazione della conformità	

¹⁰⁷ Nello specifico, il mantenimento comporta due riunioni in presenza con esperti all'anno (100 000 EUR), costi dei contraenti che partecipano all'elaborazione e alla revisione della documentazione di supporto del sistema, la diffusione dei sistemi di certificazione, il sostegno alle valutazioni tra pari e l'attuazione delle valutazioni di conformità (4 x 15 000 = 60 000 EUR). Il costo comprende anche la parte operativa della piattaforma MCE e il sito web dell'ENISA sulla certificazione (40 000 EUR).

I diritti riscossi in relazione a tale attività saranno definiti in un atto di esecuzione, a seguito dell'adozione del regolamento sulla cibersicurezza riveduto. Tuttavia, per indicare i costi stimati e le entrate previste, i calcoli sono stati effettuati sulla base di stime fornite dall'ENISA e incluse nella valutazione d'impatto della proposta di revisione del regolamento sulla cibersicurezza. I costi relativi al sostegno alle attività di verifica e valutazione sono stimati come segue:

ETP: quattro all'anno

Costi operativi: 800 000 all'anno

Costi totali: 6 500 000 milioni (5 anni); all'anno: 1 300 000 EUR

Per l'ENISA si prevedono nel primo anno investimenti una tantum, cui faranno seguito costi di mantenimento. Tali costi sarebbero gradualmente coperti dalle entrate derivanti dai diritti riscossi.

Anno	Entrate
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIMENSIONI DIGITALI

4.1. Prescrizioni di rilevanza digitale

Descrizione di alto livello delle prescrizioni di rilevanza digitale e delle relative categorie (dati, digitalizzazione dei processi e automazione, soluzioni digitali e/o servizi pubblici digitali)

Riferimento alla prescrizione	Descrizione della prescrizione	Soggetti interessati dalla prescrizione	Processi di alto livello	Categorie
Articolo 5, paragrafo 1, lettera a) Sostegno all'attuazione del diritto dell'Unione	a) prestando assistenza agli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, anche emanando orientamenti tecnici e relazioni, fornendo consulenza e condividendo le migliori pratiche, nonché agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;	- ENISA - Stati membri	- trattamento dei dati al fine di emanare orientamenti tecnici e relazioni, fornendo consulenza e condividendo le migliori pratiche, nonché agevolando lo scambio di migliori pratiche tra le autorità competenti - agevolare gli scambi di buone pratiche	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 1, lettera b) Sostegno all'attuazione del diritto dell'Unione	b) agevolando la condivisione di informazioni tra i vari settori e al loro interno, in particolare per quanto riguarda i settori elencati negli allegati I e II della direttiva (UE) 2022/2555 e i prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847, fornendo migliori pratiche e orientamenti sugli strumenti e sulle procedure disponibili	- ENISA - settori elencati negli allegati I e II della direttiva (UE) 2022/2555 - portatori di interessi sui quali coincide il regolamento (UE) 2024/2847	Fornitura di migliori pratiche e orientamenti sugli strumenti e sulle procedure disponibili per la condivisione delle informazioni	Trattamento dei dati Flusso di dati

Articolo 5, paragrafo 1, lettera c) Sostegno all'attuazione del diritto dell'Unione	c) su richiesta della Commissione, assistendo gli Stati membri mediante la fornitura di sostegno, ad esempio orientamenti tecnici, anche in merito alle misure di gestione dei rischi di cibersicurezza, strumenti per la valutazione di maturità della cibersicurezza e manuali di risposta agli incidenti , adattati ai settori elencati negli allegati I e II della direttiva (UE) 2022/2555, al fine di agevolare il miglioramento dei loro livelli di maturità della cibersicurezza e la conformità al diritto dell'Unione in materia di cibersicurezza;	- Commissione europea - ENISA - settori elencati negli allegati I e II della direttiva (UE) 2022/2555	Fornitura di orientamenti tecnici	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 1, lettera e)	e) assistendo gli Stati membri e i pertinenti soggetti dell'UE nello sviluppo e nella promozione di politiche sulla cibersicurezza che sostengano la disponibilità generale e l'integrità del carattere pubblico di una rete internet aperta, che ne costituisce l'aspetto essenziale;	ENISA Stati membri Soggetti dell'UE	Assistenza nello sviluppo e nella promozione di politiche sulla cibersicurezza	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 1, lettera f) Sostegno all'attuazione del diritto dell'Unione	f) conformemente al regolamento (UE) 2024/2847, fornendo consulenza e sostegno tecnici su questioni relative all'attuazione e all'applicazione di tale regolamento	- ENISA - portatori di interesse sui quali incide il regolamento (UE) 2024/2847	La fornitura di consulenza e sostegno tecnici richiede il trattamento e la condivisione di informazioni sui requisiti normativi, sulle difficoltà di attuazione e sugli orientamenti in materia di conformità.	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 1, lettera h)	h) su richiesta del comitato europeo per la protezione dei dati, fornendo consulenza sull'attuazione di aspetti specifici relativi alla cibersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e della vita privata.	ENISA EDPB	Fornitura di consulenza su richiesta	Trattamento dei dati Flusso di dati

Articolo 5, paragrafo 2 Contributo alle valutazioni dei rischi per la cibersicurezza a livello dell'Unione	L'ENISA contribuisce alle valutazioni coordinate a livello dell'Unione dei rischi per la cibersicurezza, comprese quelle effettuate a norma dell'articolo 22 della direttiva (UE) 2022/2555.	ENISA Stati membri Pubblico in generale	Contribuire a valutazioni coordinate dei rischi, che richiedono il trattamento dei dati e flussi di dati	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 3 L'ENISA emana orientamenti	L'ENISA emana orientamenti relativi all'interoperabilità dei sistemi informativi e di rete per la condivisione delle informazioni, anche per quanto riguarda i poli informatici transfrontalieri di cui all'articolo 6, paragrafo 3, del regolamento (UE) 2025/38.	ENISA Stati membri	L'ENISA emana orientamenti	Trattamento dei dati Flusso di dati
Articolo 5, paragrafo 5 Sostegno alla Commissione	Su richiesta della Commissione , l'ENISA fornisce competenze, consulenza tecnica, informazioni o analisi o svolge lavori preparatori su specifiche questioni di cibersicurezza al fine di orientare l'elaborazione delle politiche della Commissione e il monitoraggio dell'attuazione della legislazione dell'Unione.	Commissione europea ENISA	Preparazione e invio di informazioni alla Commissione	Trattamento dei dati Flusso di dati

Articolo 6 Sviluppo delle capacità	L'ENISA fornisce assistenza mettendo a disposizione conoscenze e competenze, migliori pratiche, ecc.	ENISA Stati membri Soggetti dell'UE Portatori di interessi pubblici e privati Autorità di vigilanza del mercato Membri dell'ECCG Centro europeo di competenza per la cibersecurity nell'ambito industriale, tecnologico e della ricerca	Fornitura di competenze e conoscenze	Trattamento dei dati Flusso di dati
Articolo 7 Sensibilizzazione e bacino di talenti	L'ENISA assiste gli Stati membri nei loro sforzi di sensibilizzazione in merito alle politiche e alla normativa dell'Unione in materia di cibersecurity e ne promuove la visibilità sviluppando strumenti e orientamenti attuabili . L'ENISA sostiene iniziative volte ad ampliare il bacino europeo di talenti nel settore della cibersecurity, in particolare attraverso il coordinamento dei concorsi.	ENISA Stati membri	Sviluppo di strumenti e orientamenti attuabili	Trattamento dei dati
Articolo 8, paragrafo 1 - Conoscenza e analisi del mercato	L'ENISA effettua e diffonde analisi delle principali tendenze del mercato della cibersecurity sia dal lato della domanda che da quello dell'offerta, in particolare per quanto riguarda i settori in cui esistono o sono previsti sistemi europei di certificazione della cibersecurity, i settori elencati negli allegati I e II della direttiva (UE) 2022/2555 e le categorie di prodotti disciplinate dal regolamento (UE) 2024/2847, compresi gli allegati III e IV di tale regolamento.	ENISA Settori elencati negli allegati I e II della direttiva (UE) 2022/2555 Categorie di prodotti contemplate dal regolamento (UE) 2024/2847	Esecuzione e diffusione di analisi	Trattamento dei dati Flusso di dati

Articolo 8, paragrafo 2 - Conoscenza e analisi del mercato	L'ENISA effettua e diffonde analisi delle tendenze tecnologiche in materia di cibersicurezza, in particolare in relazione alle attività e ai soggetti che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 e ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847.	ENISA Pubblico in generale, portatori di interessi ai sensi della direttiva (UE) 2022/2555 e del regolamento (UE) 2024/2847	Esecuzione e diffusione di analisi	Trattamento dei dati Flusso di dati
Articolo 8, paragrafo 3 - Conoscenza del mercato e sostegno agli ecosistemi	L'ENISA sviluppa conoscenze e diffonde consulenze tecniche e analisi su strumenti, norme quadro e migliori pratiche all'avanguardia in materia di cibersicurezza.	ENISA Pubblico in generale	Diffusione di consulenze tecniche e analisi su strumenti, norme quadro e migliori pratiche all'avanguardia in materia di cibersicurezza.	Trattamento dei dati Flusso di dati
Articolo 9 Cooperazione internazionale	L'ENISA fornisce il proprio contributo analizzando i risultati delle esercitazioni internazionali e comunicandoli al consiglio di amministrazione, agevolando lo scambio di migliori pratiche e fornendo alla Commissione competenze e consulenza.	Pubblico internazionale ENISA Consiglio di amministrazione dell'ENISA Commissione europea	Analisi e comunicazione; fornitura di consulenza, ecc.	Trattamento dei dati Flusso di dati
Articolo 10, paragrafi 2 e 3 Cooperazione operativa	2. L'ENISA è membro della rete di CSIRT nazionali istituita a norma dell'articolo 15, paragrafo 1, della direttiva (UE) 2022/2555 e ne assicura il segretariato a norma dell'articolo 15, paragrafo 2, della direttiva (UE) 2022/2555.	ENISA CSIRT (articolo 15, paragrafo 1, della direttiva (UE) 2022/2555) EU-CyCLONe (articolo 16, paragrafo 2, della direttiva (UE)	Facilitare lo scambio di informazioni, assumere le funzioni di segretariato della rete	Flusso di dati Soluzione digitale Servizio pubblico

	3. L'ENISA assicura il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) a norma dell'articolo 16, paragrafo 2, secondo comma, della direttiva (UE) 2022/2555.	2022/2555)		digitale
Articolo 11, paragrafo 1, lettera b) Conoscenza situazionale Articolo 12 Allerte precoci	Emissione di allerte precoci in conformità dell'articolo 12	Commissione europea ENISA Europol EU-CyCLONe Rete di CSIRT CERT-UE Soggetti elencati negli allegati I e II della direttiva (UE) 2022/2555	Emissione di allerte precoci	Trattamento dei dati Flusso di dati Servizio pubblico digitale
Articolo 10, paragrafo 4, lettera b) Cooperazione operativa	b) su richiesta di uno o più Stati membri, fornire consulenza e valutazioni in relazione a uno specifico incidente informatico o una specifica minaccia informatica , potenziale o in corso, anche tramite la messa a disposizione di competenze e l' agevolazione della gestione tecnica di tali incidenti , e il sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri	ENISA Stati membri	Fornitura di consulenza e valutazioni in relazione a uno specifico incidente informatico o una specifica minaccia informatica, potenziale o in corso; agevolazione della gestione tecnica di tali incidenti; sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri	Trattamento dei dati Flusso di dati Servizi pubblici digitali

Articolo 10, paragrafo 4, lettera c) Cooperazione operativa	c) effettuare analisi delle vulnerabilità, delle minacce e degli incidenti	ENISA Stati membri	Raccolta di dati da fonti pubbliche e scambio di dati con gli Stati membri	Trattamento dei dati Flusso di dati
Articolo 10, paragrafo 4, lettera d) Cooperazione operativa	d) su richiesta di uno o più Stati membri, fornire sostegno in relazione a indagini tecniche ex post sugli incidenti significativi ai sensi della direttiva (UE) 2022/2555	ENISA Stati membri	Analisi e sostegno in risposta a indagini tecniche sugli incidenti	Trattamento dei dati Flusso di dati
Articolo 10, paragrafo 4, lettera e) Cooperazione operativa	e) contribuire a sostenere la gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello operativo, in particolare assistendo EU-CyCLONe nella redazione di relazioni a livello politico e agevolando la condivisione tempestiva delle informazioni tra la rete di CSIRT e EU-CyCLONe	ENISA EU-CyCLONe Rete di CSIRT	Analisi dei dati a sostegno della redazione delle relazioni; agevolazione della condivisione tempestiva delle informazioni tra le reti	Trattamento dei dati Flusso di dati Servizio pubblico digitale
Articolo 10, paragrafo 5 Cooperazione operativa	Su richiesta di uno Stato membro o di un soggetto dell'Unione in cooperazione con il CERT-UE, l'ENISA sostiene una comunicazione pubblica coerente in merito a un incidente o a una minaccia informatica.	ENISA Stati membri	Ricezione di richieste ed eventuale comunicazione	Flusso di dati

Articolo 10, paragrafo 6 Cooperazione operativa	L'ENISA sostiene la cooperazione tra gli Stati membri e attraverso il CERT-UE tra i soggetti dell'Unione per quanto riguarda la diffusione di strumenti di comunicazione sicura . Nell'ambito della rete dei CSIRT e di EU-CyCLONe l'ENISA usa strumenti di comunicazione sicura forniti da soggetti giuridici che non sono stabiliti in paesi terzi o che non sono controllati da paesi terzi o da cittadini di paesi terzi.	ENISA Commissione europea Stati membri Soggetti dell'UE Rete di CSIRT EU-CyCLONe	Sostegno alla diffusione di strumenti di comunicazione sicura e utilizzo di tali strumenti nell'ambito della rete di CSIRT e di EU-CyCLONe.	Soluzione digitale Servizio pubblico digitale
Articolo 11, paragrafo 1, lettera a) Conoscenza situazionale condivisa in materia di cibersicurezza	a) sviluppare , in cooperazione con EU-CyCLONe, la rete di CSIRT, la Commissione, il CERT-UE, Europol e altri soggetti pertinenti dell'Unione, archivi di intelligence verificata e affidabile sulle minacce informatiche, comprese le tendenze in materia di incidenti, tattiche, tecniche e procedure	Commissione europea ENISA EU-CyCLONe Rete di CSIRT Europol Soggetti dell'UE CERT-UE	Sviluppo di archivi	Flusso digitale Soluzione digitale Servizio pubblico digitale
Articolo 11, paragrafo 1, lettere da c) a g) Conoscenza situazionale condivisa in materia di cibersicurezza	Fornire tempestivamente analisi ad hoc (alcune su richiesta); fornire analisi e consulenza tecnica; elaborare una relazione sulla situazione tecnica in cooperazione con altri soggetti; monitorare le tendenze e condividerle	ENISA Stati membri Commissione europea Soggetti dell'UE EU-CyCLONe Rete di CSIRT	Analisi dei dati, condivisione di informazioni e presentazione di relazioni (alcune su richiesta)	Trattamento dei dati Flusso di dati

Articolo 11, paragrafo 2, lettera a) Conoscenza situazionale condivisa in materia di cibersecurity	L'ENISA effettua analisi delle minacce informatiche, degli incidenti, delle tendenze, delle tecnologie emergenti e del loro impatto, compresa un' analisi periodica riguardante i settori elencati negli allegati I e II della direttiva (UE) 2022/2555 e le pertinenti categorie di prodotti disciplinate dal regolamento (UE) 2024/2847	ENISA Pubblico in generale	Analisi dei dati per fornire informazioni rilevanti per la cibersecurity; relazione periodica	Trattamento dei dati Flusso di dati
Articolo 11, paragrafo 2, lettera b) Conoscenza situazionale condivisa in materia di cibersecurity	L'ENISA fornisce, in cooperazione con la Commissione e, se del caso, con la rete di CSIRT, consulenza, orientamenti e migliori pratiche per la sicurezza dei sistemi informativi e di rete, in particolare per la sicurezza delle infrastrutture su cui poggiano i settori di cui agli allegati I e II della direttiva (UE) 2022/2555	Commissione europea CERT-UE Rete di CSIRT Pubblico in generale	Fornitura di consulenza, orientamenti e migliori pratiche	Trattamento dei dati Flusso di dati
Articolo 11, paragrafo 2, lettera c) Conoscenza situazionale condivisa in materia di cibersecurity	L'ENISA effettua analisi strategiche a lungo termine delle minacce informatiche e degli incidenti al fine di individuare le tendenze emergenti e contribuire a prevenire gli incidenti.	ENISA Pubblico in generale	Analisi dei dati e individuazione delle minacce emergenti	Trattamento dei dati
Articolo 11, paragrafo 3 Conoscenza situazionale condivisa in materia di cibersecurity	L'ENISA può rendere pubbliche le analisi , le consulenze, gli orientamenti, le migliori pratiche e le relazioni di cui al paragrafo 2, in accordo con i soggetti che vi hanno contribuito di cui al paragrafo 2.	ENISA Pubblico in generale	Rendere pubbliche le informazioni	Flusso di dati Servizio pubblico digitale

Articolo 13, paragrafo 2 Sostegno nella risposta agli incidenti	2. Su richiesta della Commissione o di EU-CyCLONe, l'ENISA, con il sostegno della rete di CSIRT e con l'approvazione dello Stato membro interessato, riesamina e valuta gli incidenti di cibersecurity significativi o gli incidenti di cibersecurity su vasta scala conformemente all'articolo 21 del regolamento (UE) 2025/38.	Commissione europea ENISA EU-CyCLONe Rete di CSIRT Stati membri	Riesame e valutazione degli incidenti di cibersecurity significativi	Trattamento dei dati
Articolo 14, paragrafo 2 Esercitazioni di cibersecurity a livello dell'Unione	2. L'ENISA mantiene un archivio degli insegnamenti tratti dalle esercitazioni di cui al paragrafo 1 e formula raccomandazioni rivolte agli Stati membri e, se del caso, ai soggetti dell'Unione in merito a come mettere in pratica in modo efficace ed efficiente tali insegnamenti.	ENISA Stati membri Soggetti dell'UE	Mantenimento di un archivio	Trattamento dei dati Soluzione digitale Servizio pubblico digitale
Articolo 14 Esercitazioni di cibersecurity a livello dell'Unione	Su richiesta di EU-CyCLONe, della Commissione, degli Stati membri o del CERT-UE, l'ENISA organizza esercitazioni di cibersecurity o vi contribuisce. L'ENISA assiste la Commissione nell'elaborazione di un programma continuo annuale di esercitazioni di cibersecurity a livello dell'Unione.	ENISA Commissione Stati membri Soggetti dell'UE CERT-UE	Ricezione di richieste di organizzazione o sostegno all'organizzazione di esercitazioni	Flusso di dati Trattamento dei dati

Articolo 15 Fornitura di strumenti e piattaforme	1. L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, comprese le piattaforme relative alla cibersicurezza a livello dell'Unione, in particolare la piattaforma unica di segnalazione degli incidenti istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 [e il punto di accesso unico istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555], nonché strumenti di prova a sostegno dell'attuazione delle procedure di valutazione della conformità a norma della pertinente normativa dell'Unione. 2. Ove opportuno, ai fini del paragrafo 1, L'ENISA coopera e scambia informazioni con la rete di CSIRT e, se del caso, con le autorità di vigilanza del mercato.	ENISA Rete di CSIRT Pubblico in generale Autorità di vigilanza del mercato	L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, quali le piattaforme	Soluzione digitale Servizio pubblico digitale Flusso di dati
Articolo 16, paragrafo 2 Servizi di gestione delle vulnerabilità	a) mantenere la banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555; b) fornire servizi di gestione delle vulnerabilità ai portatori di interessi, basandosi sulla banca dati europea delle vulnerabilità e utilizzando le informazioni pertinenti di cui dispone l'ENISA; c) se del caso, avviare una cooperazione strutturata con organizzazioni che forniscono programmi, registri o banche dati simili alla banca dati europea delle vulnerabilità; d) assistere attivamente i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555 per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere	ENISA CSIRT nazionali Rete di CSIRT Autorità nazionali competenti Industria Comunità della ricerca Pubblico in generale Soggetti internazionali che forniscono programmi, registri o banche dati	Fornitura di servizi di gestione delle vulnerabilità; se del caso, avvio di una cooperazione strutturata; cooperazione con i portatori di interessi	Soluzione digitale Servizio pubblico digitale Flusso di dati

	un impatto significativo su soggetti in più di uno Stato membro; e) sviluppare e mantenere metodologie e meccanismi di governance per l'individuazione e la divulgazione coordinata delle vulnerabilità, in cooperazione con le autorità nazionali competenti, i CSIRT, l'industria e la comunità della ricerca			
Articolo 17 Certificazione della cbersicurezza Articolo 18 Normazione, specifiche tecniche e orientamenti	Articolo 17, paragrafo 1 a) preparare proposte di sistemi europei di certificazione della cbersicurezza ("proposte di sistemi") per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cbersicurezza dei soggetti e le relative specifiche tecniche conformemente all'articolo 74; b) mantenere i sistemi europei di certificazione della cbersicurezza adottati conformemente all'articolo 75, anche in considerazione di un'eventuale revisione di tali sistemi a norma dell'articolo 76; c) promuovere la diffusione dei sistemi adottati e gestire un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cbersicurezza, sui certificati europei di cbersicurezza e sulle dichiarazioni UE di conformità e li pubblicizza conformemente all'articolo 79 Articolo 17, paragrafo 2 e) elaborazione di disposizioni tipo cui fare riferimento nei sistemi europei di certificazione della cbersicurezza ("proposte di sistemi") per i prodotti TIC, i servizi TIC, i processi TIC, i	ENISA Pubblico in generale	Analisi di dati e scambio dei flussi di dati con la Commissione e gli altri portatori di interessi; preparazione della proposta di sistema di certificazione; gestione del sito web dell'ENISA	Trattamento dei dati Flussi di dati Servizio pubblico digitale

	servizi di sicurezza gestiti e la postura di cibersicurezza dei soggetti a norma dell'articolo 81, paragrafo 5. Articolo 18 1. L'ENISA elabora specifiche tecniche e orientamenti a sostegno dell'attuazione della legislazione dell'Unione nel settore della cibersicurezza. 2. L'ENISA monitora le attività di elaborazione della normazione a livello dell'Unione e, conformemente all'articolo 9, a livello internazionale e vi partecipa anche assumendo un ruolo guida. 3. L'ENISA contribuisce allo sviluppo e alla valutazione di algoritmi crittografici. Qualora un algoritmo crittografico valutato sia valutato positivamente, l'ENISA coopera, conformemente al regolamento (UE) n. 1025/2012, con gli organismi europei di normazione per sostenerne la normazione. 4. L'ENISA fornisce competenze tecniche alla Commissione e all'ECCG in merito a norme o specifiche tecniche adeguate a sostegno delle politiche dell'Unione in materia di cibersicurezza, in particolare il regolamento (UE) 2024/2847, anche per quanto riguarda la normativa di armonizzazione dell'Unione nel settore della cibersicurezza e i sistemi europei di certificazione della cibersicurezza a norma dell'articolo 81, paragrafo 1, lettera d). 5. L'ENISA assiste la Commissione nella valutazione dei progetti di norme armonizzate a sostegno dell'attuazione della normativa di			
--	---	--	--	--

	armonizzazione dell'Unione nel settore della cibersecurity.			
Articolo 19 – Quadro europeo delle competenze in materia di cibersecurity	L'ENISA sviluppa e rende pubblicamente disponibile un quadro europeo delle competenze in materia di cibersecurity ("ECSF") . Prima di rendere l'ECSF pubblicamente disponibile o di aggiornarlo a norma del paragrafo 4, l'ENISA consulta la Commissione . L'uso dell'ECSF da parte dei soggetti pubblici e privati ha carattere volontario . L'ENISA può consultare i portatori di interessi per quanto riguarda lo sviluppo e la diffusione dell'ECSF.	ENISA Commissione Pubblico in generale Stati membri Soggetti dell'UE Portatori di interessi pubblici e privati	Mantenimento dell'ECSF; consultazione dei portatori di interessi; diffusione dell'ECSF	Trattamento dei dati Flusso di dati Soluzione digitale
Articoli da 20 a 23 – Sistemi europei di attestazione delle competenze individuali in materia di cibersecurity	L'ENISA sviluppa, adotta e mantiene sistemi europei di attestazione delle competenze individuali in materia di cibersecurity . L'uso di sistemi europei di attestazione delle competenze individuali in materia di cibersecurity è volontario per gli organismi pubblici nazionali e i soggetti privati , salvo diversamente specificato dal diritto nazionale. Prima di avviare un nuovo sistema europeo di attestazione delle competenze individuali in materia di cibersecurity, l'ENISA consulta la Commissione . L'ENISA adotta tale sistema solo di previo parere positivo della Commissione . Nella fase di elaborazione di un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity, l'ENISA può consultare i portatori di interessi pertinenti .	ENISA Commissione Pubblico in generale Stati membri Soggetti dell'UE Portatori di interessi pubblici e privati (che contribuiscono allo sviluppo di un sistema di attestazione; richiedenti e fornitori di attestati europei delle competenze individuali in materia di cibersecurity, compresi i valutatori)	Sviluppo e mantenimento dei sistemi; consultazioni dei portatori di interessi; trattamento delle domande; adozione di decisioni; gestione di un sito web	Trattamento dei dati Flusso di dati Soluzione digitale Servizio pubblico digitale

	L'ENISA assicura una stretta cooperazione con gli Stati membri durante l'intera fase di preparazione dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza. I fornitori autorizzati di attestati valutano se gli interessati soddisfano i requisiti di un sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza e, qualora tali requisiti siano soddisfatti, rilasciano attestati europei delle competenze individuali in materia di cibersicurezza. L'ENISA fornisce orientamenti ai valutatori e impartisce loro una formazione obbligatoria in merito ai requisiti e ai metodi di valutazione previsti nel sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza di cui all'articolo 20, paragrafo 3, lettera b). I soggetti che intendono diventare fornitori autorizzati di attestati o rinnovare la propria autorizzazione ("richiedenti") presentano una domanda all'ENISA. I fornitori autorizzati di attestati garantiscono che, su richiesta dell'interessato, gli attestati europei delle competenze individuali in materia di cibersicurezza siano rilasciati sotto forma di attestati elettronici di attributi in un formato che può essere archiviato nei portafogli europei di identità digitale di cui al regolamento (UE) n. 910/2014. I richiedenti e i fornitori autorizzati di attestati consentono all'ENISA di effettuare valutazioni nell'ambito della procedura di domanda iniziale.			
--	---	--	--	--

	del mantenimento dell'autorizzazione o del suo rinnovo e di condividere tutte le informazioni pertinenti per garantire che i requisiti di cui ai paragrafi 3 e 4 o gli obblighi di cui al paragrafo 5 siano soddisfatti o continuino a essere soddisfatti conformemente all'articolo 22, paragrafo 2. I fornitori autorizzati di attestati informano immediatamente l'ENISA se uno dei requisiti di cui al paragrafo 3 non è più soddisfatto o se sorgono dubbi in merito al fatto che tali requisiti siano soddisfatti, anche per quanto riguarda l'indipendenza dei valutatori. I richiedenti versano un diritto all'ENISA per la valutazione della loro domanda. I fornitori autorizzati di attestati versano un diritto all'ENISA per il mantenimento della loro autorizzazione. L'ENISA valuta se i requisiti di cui all'articolo 21, paragrafi 3 e 4, e gli obblighi di cui all'articolo 21, paragrafo 5, sono soddisfatti o continuano a essere soddisfatti dai richiedenti e dai fornitori autorizzati di attestati. Dopo aver esaminato una domanda alla luce dei requisiti di cui all'articolo 21, paragrafi 3 e 4, l'ENISA può adottare una decisione. L'ENISA può modificare, sospendere o revocare tali decisioni. L'ENISA gestisce e aggiorna regolarmente un apposito sito web dedicato che fornisce informazioni pubbliche riguardanti:			
--	--	--	--	--

	a) l'ECSF, comprendenti il quadro e il relativo calendario di aggiornamento; b) i sistemi europei di attestazione delle competenze individuali in materia di cibersecurity, i progressi compiuti e le tempistiche per il loro sviluppo; c) i diritti associati a ciascun sistema europeo di attestazione delle competenze individuali in materia di cibersecurity adottato a norma dell'articolo 47 del presente regolamento; d) il costo indicativo di un attestato europeo delle competenze individuali in materia di cibersecurity a norma dell'articolo 20, paragrafo 4; e) l'elenco dei fornitori autorizzati di attestati.			
--	--	--	--	--

Articolo 25 Composizione del consiglio di amministrazione	Nomina dei membri del consiglio di amministrazione dell'ENISA.	ENISA Commissione europea Stati membri	Nomina dei membri	Flusso di dati Trattamento dei dati
Articolo 28, paragrafo 1 Funzioni del consiglio di amministrazione Articolo 30 Comitato esecutivo	b. adotta il progetto di documento unico di programmazione dell'ENISA di cui all'articolo 44 prima che sia trasmesso alla Commissione per un parere; f) valuta e adotta la relazione annuale consolidata sulle attività dell'ENISA, inclusi i conti e una descrizione di come l'ENISA ha conseguito i propri indicatori di risultato, trasmette, entro il 1° luglio dell'anno successivo, sia la relazione annuale che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti europea; rende pubblica la relazione annuale; i) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti da relazioni di revisione contabile e valutazioni interne ed esterne e dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalla Procura europea (EPPO);	ENISA Commissione europea Parlamento europeo Consiglio dell'UE Corte dei conti Stati membri Pubblico in generale	Presentazione del documento unico di programmazione alla Commissione per parere; valutazione e adozione della relazione annuale consolidata sulle attività dell'ENISA, inclusi i conti e una descrizione di come l'ENISA ha conseguito i propri indicatori di risultato; trasmissione sia della relazione annuale che della sua valutazione; seguito dato alle risultanze	Flusso di dati Trattamento dei dati

Articolo 31, paragrafo 8 Nomina, rimozione dall'incarico e proroga del mandato	Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo ad norma del paragrafo 6. Entro i tre mesi che precedono tale proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.	ENISA Consiglio di amministrazione dell'ENISA Parlamento europeo	Il consiglio di amministrazione informa il Parlamento europeo	Flusso di dati
Articolo 32, paragrafo 3 Compiti e responsabilità del direttore esecutivo Articolo 32, paragrafo 5	3. Su richiesta, il direttore esecutivo riferisce al Parlamento europeo sullo svolgimento dei suoi compiti. Il Consiglio può invitare il direttore esecutivo a riferire sullo svolgimento dei suoi compiti. Prepara i progetti di piani di bilancio, le strategie, i documenti strategici.	Direttore esecutivo dell'ENISA Parlamento europeo	Comunicazione delle prestazioni	Flusso di dati Trattamento dei dati
Articolo 35, paragrafi 5 e 6 Gruppo consultivo ENISA	5. Il gruppo consultivo ENISA fornisce consulenza all'ENISA relativamente allo svolgimento dei suoi compiti, tranne per quanto concerne l'applicazione delle disposizioni dei titoli III, IV e V del presente regolamento. In particolare, esso consiglia il direttore esecutivo ai fini della stesura di una proposta relativa al programma di lavoro annuale dell'ENISA e della comunicazione con i relativi portatori di interessi sulle questioni inerenti al programma di lavoro annuale. 6. Il gruppo consultivo ENISA informa periodicamente il consiglio di amministrazione sulle sue attività.	ENISA Membri del gruppo consultivo ENISA Consiglio di amministrazione dell'ENISA Direttore esecutivo dell'ENISA	Fornitura di consulenza e informazioni sulle proprie attività	Trattamento dei dati Flusso di dati

Articoli da 36 a 43 Commissione di ricorso	L'ENISA istituisce una commissione di ricorso con decisione del consiglio di amministrazione. La commissione di ricorso è composta da un presidente e da altri tre membri. Ciascun membro della commissione di ricorso ha un supplente. Il supplente rappresenta il membro assente. Il consiglio di amministrazione nomina il presidente, gli altri membri e i loro supplenti in base a un elenco di candidati idonei predisposto dalla Commissione. L'elenco dei candidati idonei è valido per un periodo di quattro anni. La validità di tale elenco può essere prorogata dal consiglio di amministrazione per ulteriori periodi di quattro anni su proposta della Commissione. Qualora ne ravvisi la necessità per la natura stessa del ricorso, la commissione di ricorso può chiedere al consiglio di amministrazione di nominare due ulteriori membri e i relativi supplenti sulla base dell'elenco di cui al paragrafo 3. La commissione di ricorso adotta e pubblica il proprio regolamento interno. Se, per uno dei motivi di cui al paragrafo 1 o per qualsivoglia altro motivo, un membro della commissione di ricorso ritiene di doversi astenere dal partecipare ad un procedimento di ricorso, ne informa la commissione stessa. Nei casi di cui ai paragrafi 2 e 3, la commissione di ricorso decide come procedere senza la partecipazione del membro interessato. Ai fini della decisione, il membro interessato è sostituito nella commissione di ricorso dal suo	ENISA Consiglio di amministrazione dell'ENISA Commissione Commissione di ricorso ai sensi dell'articolo 36 della proposta relativa al regolamento sulla cibersicurezza 2 Richiedenti (persone giuridiche che intendono diventare fornitori autorizzati di attestati, mantenere o rinnovare la loro autorizzazione)	Adozione di decisioni sulla base di ricorsi Trattamento dei ricorsi Preparazione e pubblicazione del regolamento interno Flussi di informazioni	Trattamento dei dati Flusso di dati Servizio pubblico digitale
---	--	---	---	---

	supplente. Il ricorso proposto a norma del paragrafo 1 è oggetto di una revisione precontenziosa conformemente all'articolo 41 prima di essere sottoposto all'esame della commissione di ricorso. I richiedenti ai sensi dell'articolo 21, paragrafo 3, possono presentare ricorso: avverso una decisione dell'ENISA nei loro confronti, a norma dell'articolo 22, paragrafo 3, o per quanto riguarda la mancata azione dell'ENISA entro i termini applicabili di cui all'articolo 22, paragrafo 4, relativamente a una domanda da essi presentata all'ENISA. Nel caso di cui al paragrafo 1, lettera a), il ricorso, insieme a una memoria che ne precisi i motivi, è presentato per iscritto conformemente al regolamento interno di cui all'articolo 36, paragrafo 5, entro due mesi dalla notifica della decisione al richiedente interessato o, in assenza di tale notifica, dal giorno in cui il richiedente è venuto a conoscenza della decisione. Nel caso di cui al paragrafo 1, lettera b), il ricorso è presentato all'ENISA per iscritto conformemente al regolamento interno di cui all'articolo 36, paragrafo 5, entro due mesi dal giorno della scadenza del termine di cui all'articolo 22, paragrafo 4. Qualora ritenga che il ricorso sia ammissibile e fondato, l'ENISA rettifica la decisione o la carenza di cui all'articolo 40, paragrafo 1. Qualora non rettifichi la decisione entro un mese dal ricevimento del ricorso, l'ENISA decide immediatamente se sospendere l'applicazione			
--	--	--	--	--

	della sua decisione e deferisce il ricorso in oggetto alla commissione di ricorso. La commissione di ricorso decide se accogliere o respingere il ricorso entro tre mesi dalla sua presentazione. Nell'esame di un ricorso, la commissione di ricorso agisce entro i termini stabiliti nel proprio regolamento interno. Ogniquale volta sia necessario, invita le parti del procedimento di ricorso a presentare, entro un dato termine, osservazioni sulle sue notifiche o sulle comunicazioni effettuate dalle altre parti del procedimento di ricorso. Le parti del procedimento di ricorso possono presentare osservazioni orali. Se constatata la fondatezza dei motivi del ricorso, la commissione di ricorso rinvia il caso all'ENISA. Quest'ultima adotta la decisione definitiva conformemente alle conclusioni della commissione di ricorso e fornisce una motivazione. L'ENISA informa di conseguenza le parti del procedimento di ricorso. È possibile presentare alla Corte di giustizia dell'Unione europea ricorsi per l'annullamento di decisioni dell'ENISA adottate a norma dell'articolo 22, paragrafo 3, o per carenza entro i termini applicabili a norma dell'articolo 22, paragrafo 4, dopo che sia stata esperita la procedura di ricorso all'interno dell'ENISA di cui agli articoli da 39 a 42 o in assenza di un intervento entro il termine applicabile a norma dell'articolo 41, paragrafo 2. L'ENISA adotta tutti i provvedimenti necessari per conformarsi alla sentenza della Corte di giustizia dell'Unione europea			
--	---	--	--	--

Articolo 44 Documento unico di programmazione	2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti dalla Commissione, predispone un progetto di documento unico di programmazione, di cui al paragrafo 1, con la corrispondente pianificazione delle risorse finanziarie e umane, conformemente all'articolo 32 del regolamento delegato (UE) 2019/715 della Commissione. 3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1, tenendo conto del parere della Commissione di cui all'articolo 32, paragrafo 7, del regolamento delegato (UE) 2019/715. Qualora decida di non tener conto di un elemento del parere della Commissione, il consiglio di amministrazione fornisce una giustificazione dettagliata per tale decisione. Il consiglio di amministrazione trasmette il documento unico di programmazione al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, unitamente a eventuali successive versioni aggiornate di tale documento.	Direttore esecutivo dell'ENISA Consiglio di amministrazione dell'ENISA Commissione europea Parlamento europeo Consiglio	Stesura, adozione e trasmissione, con cadenza annuale, di un documento unico di programmazione	Flusso di dati
Articolo 45 Formazione del bilancio dell'ENISA	4. La Commissione trasmette il progetto di stato di previsione all'autorità di bilancio insieme al progetto di bilancio generale dell'Unione. Il progetto di stato di previsione è altresì messo a disposizione dell'ENISA.	ENISA Commissione europea	Scambio di informazioni	Flusso di dati

Articolo 47 Diritti	In relazione alle attività nell'ambito dei sistemi europei di attestazione individuale di cui all'articolo 22, paragrafo 1, i seguenti diritti sono riscossi presso i richiedenti ai sensi dell'articolo 21, paragrafo 3, o presso i fornitori autorizzati di attestati, per contribuire a coprire integralmente i costi delle attività svolte dall'ENISA: a. rilascio di autorizzazioni in seguito all'esame dei requisiti di cui all'articolo 21, paragrafi 3 e 4, compresa l'esecuzione di valutazioni; b. mantenimento annuale dell'autorizzazione; c. rinnovo delle autorizzazioni per i fornitori di attestati europei delle competenze individuali in materia di cibersicurezza, compresa l'esecuzione di valutazioni. In relazione alla certificazione, i seguenti diritti sono riscossi presso gli organismi di valutazione della conformità per il mantenimento dei sistemi europei di certificazione della cibersicurezza nell'ambito dei quali sono rilasciati i certificati europei di cibersicurezza, in particolare: - un diritto annuale per la partecipazione a un sistema europeo di certificazione della cibersicurezza; - un diritto per il rilascio dei certificati europei di cibersicurezza nell'ambito dei sistemi europei di certificazione della cibersicurezza. I diritti di cui alla lettera b) sono riscossi quando l'organismo di valutazione della conformità	Commissione ENISA Fornitori di attestati Organismi di valutazione della conformità	Informazioni sul trattamento; pagamento dei diritti; relazione sui diritti	Trattamento dei dati Flusso di dati
--------------------------------	--	---	---	--

	trasmette i certificati europei di cibersecurity all'ENISA ai fini della pubblicazione sul sito web di quest'ultima a norma dell'articolo 79. La Commissione adotta atti di esecuzione che stabiliscono norme dettagliate relative ai diritti riscossi dall'ENISA. L'ENISA include una relazione sui diritti riscossi e sulla loro incidenza sul bilancio dell'Agenzia nell'ambito della procedura di rendicontazione.			
Articolo 48 Articolo 49 Incidenza sul bilancio	Articolo 48 3. Il direttore esecutivo trasmette ogni anno all'autorità di bilancio tutte le informazioni pertinenti ai risultati delle procedure di valutazione. Articolo 49 1. Il contabile dell'ENISA comunica i conti provvisori per l'esercizio (anno N) al contabile della Commissione e alla Corte dei conti entro il 1° marzo dell'esercizio successivo (anno N + 1). 2. Il contabile dell'ENISA comunica inoltre al contabile della Commissione le informazioni contabili necessarie ai fini del consolidamento, secondo le modalità e il formato stabiliti da quest'ultimo, entro il 1° marzo dell'anno N + 1. 3. L'ENISA trasmette al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti una relazione sulla gestione finanziaria e di bilancio dell'anno N entro il 31 marzo dell'anno N + 1. 4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti	ENISA Consiglio di amministrazione dell'ENISA Commissione europea Consiglio Parlamento europeo	Elaborazione e condivisione delle informazioni relative al bilancio dell'ENISA.	Trattamento dei dati Flusso di dati

	provvisori dell'ENISA per l'anno N, il contabile dell'Agenzia redige i conti definitivi dell'ENISA. 5. Il consiglio di amministrazione formula un parere sui conti definitivi dell'ENISA per l'anno N. Il contabile dell'Agenzia redige i conti definitivi dell'ENISA sotto la propria responsabilità. Il direttore esecutivo li presenta al consiglio di amministrazione per parere.			
Articolo 52 Dichiarazione di interessi	Le parti rendono una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza.	Dirigenza dell'ENISA (direttore esecutivo, vicedirettore esecutivo); Consiglio di amministrazione Esperti nazionali distaccati	Trattamento e condivisione dei dati sulla dichiarazione di interessi	Trattamento dei dati Flusso di dati
Articolo 58 Funzionari di collegamento	1. Ciascuno Stato membro designa almeno due funzionari di collegamento [della propria autorità nazionale per la cibersicurezza] quali esperti nazionali distaccati presso l'ENISA affinché prestino servizio nella sede o nell'ufficio locale di quest'ultima, in conformità dell'articolo 59, paragrafo 2. Anche la Commissione può designare un funzionario di collegamento. 2. I funzionari di collegamento designati dai rispettivi Stati membri hanno la facoltà di	ENISA Stati membri	Designazione dei funzionari di collegamento e condivisione delle informazioni	Trattamento dei dati Flusso di dati

	richiedere e ricevere da questi ultimi tutte le informazioni pertinenti , come previsto dal presente regolamento, nel pieno rispetto del diritto nazionale o della prassi vigente nei rispettivi Stati membri, in particolare per quanto riguarda la protezione dei dati e le regole di riservatezza.			
Articolo 67 Gestione di informazioni classificate	Prevvia consultazione della Commissione , l'ENISA adotta regole in materia di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni sensibili non classificate e delle ICUE di cui alle decisioni (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444. Le regole in materia di sicurezza dell'ENISA includono le disposizioni che disciplinano lo scambio, il trattamento e la conservazione di tali informazioni.	ENISA Consiglio di amministrazione Commissione	Gestione di informazioni classificate	Trattamento dei dati Flusso di dati
Articoli 68, 69 e 70 Cooperazione con i soggetti dell'Unione e le autorità nazionali Cooperazione con i portatori di interessi Cooperazione con paesi terzi	L'ENISA coopera e scambia informazioni su questioni relative alla cibersecurity con i soggetti pertinenti dell'Unione, le autorità di vigilanza del mercato e le autorità di controllo, i pertinenti portatori di interessi, le autorità competenti di paesi terzi o le organizzazioni internazionali	ENISA Europol Centro europeo di competenza per la cibersecurity nell'ambito industriale, tecnologico e della ricerca Comitato europeo per la protezione dei dati Pubblico in generale Consiglio	Scambio di informazioni	Flusso di dati

Articolo 72 - Informazione e consultazione del pubblico sui sistemi europei di certificazione della cibersecurity	2. La Commissione gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni sui seguenti aspetti: a) sistemi europei di certificazione della cibersecurity di cui è stato richiesto lo sviluppo; b) priorità strategiche per l'armonizzazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o dei requisiti di sicurezza della normativa dell'Unione, compresi i potenziali settori per i quali potrebbe essere richiesto un sistema europeo di certificazione della cibersecurity. 3. La Commissione rende pubbliche sul sito web di cui al paragrafo 2 del presente articolo le informazioni concernenti la sua richiesta all'ENISA relativa alla preparazione di una proposta di sistema di cui all'articolo 73 e la sua decisione di accogliere, respingere o abbandonare la proposta di sistema trasmessa dall'ENISA in conformità dall'articolo 74, paragrafo 7.	Commissione europea Pubblico in generale ENISA	Gestione del sito web informativo, che impone alla Commissione di fornire informazioni su un sito web accessibile al pubblico e di predisporre le relative attività di gestione dei dati su base continuativa.	Servizio pubblico digitale Soluzione digitale
Articolo 72 - Informazione e consultazione del pubblico sui sistemi europei di certificazione della cibersecurity	Nel corso della preparazione di una proposta di sistema da parte dell'ENISA a norma dell'articolo 74, il Parlamento europeo e il Consiglio possono chiedere alla Commissione, in qualità di presidente dell'ECCG, e all'ENISA di presentare le pertinenti informazioni relative a un progetto di proposta di sistema. Su richiesta del Parlamento europeo o del Consiglio, l'ENISA, d'intesa con la Commissione e fatto salvo l'articolo 54, può mettere a disposizione del Parlamento europeo e del Consiglio le parti pertinenti di un	ENISA Consiglio dell'UE Parlamento europeo	Richiesta e invio di informazioni su un progetto di proposta di sistema elaborato dall'ENISA	Flussi di dati

	progetto di proposta di sistema con modalità adeguate al livello di riservatezza richiesto e, se del caso, limitate. Il Parlamento europeo e il Consiglio possono invitare la Commissione e l'ENISA a discutere questioni relative all'attuazione dei sistemi europei di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti.			
Articolo 73 Richiesta di un sistema europeo di certificazione della cibersecurity Articolo 74 Preparazione e adozione dei sistemi europei di certificazione della cibersecurity (articolo 17)	Articolo 73 1. La Commissione può chiedere all'ENISA di preparare una proposta di sistema europeo di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti. In casi debitamente giustificati, l'ECCG può suggerire alla Commissione di presentare una richiesta di cui al paragrafo 1. 4. Nel preparare la richiesta di cui al paragrafo 1, la Commissione consulta debitamente l'ENISA e l'ECCG e tiene conto delle opinioni di tutti i pertinenti portatori di interessi e di altri soggetti dell'Unione compresi, se del caso, quelli pertinenti ai sensi della normativa dell'Unione in base alla quale un sistema europeo di certificazione della cibersecurity conferisce una presunzione di conformità. Articolo 74 3. In sede di preparazione della proposta di	Commissione europea ENISA ECCG Portatori di interessi esperti	Preparazione di una richiesta e di un sistema di certificazione e relativa consultazione dei portatori di interessi	Trattamento dei dati Flussi di dati Servizio pubblico digitale (articolo 17)

	sistema, l'ENISA coopera strettamente con l'ECCG. L'ECCG fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e, se del caso, delle relative specifiche tecniche. L'ENISA chiede ai membri dell'ECCG di fornire un parere scritto sulla proposta di sistema. 4. L'ENISA consulta tempestivamente i portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo. L'ENISA coopera inoltre con le autorità pubbliche competenti degli Stati membri e con i pertinenti soggetti dell'Unione per ricevere una consulenza specialistica in relazione alla preparazione della proposta di sistema e, se del caso, delle relative specifiche tecniche. 6. L'ENISA trasmette la proposta di sistema alla Commissione entro 60 giorni dalla data della richiesta di cui al paragrafo 5. 7. Quando riceve la proposta di sistema, la Commissione valuta se il sistema corrisponda alla richiesta presentata a norma dell'articolo 73. 8. Se la Commissione rinvia una proposta di sistema all'ENISA per revisione conformemente al paragrafo 7, lettera b), si applicano di conseguenza i paragrafi 4, 5 e 7.			
--	---	--	--	--

Articolo 75 Mantenimento di un sistema europeo di certificazione della cibersecurity	2. L'ENISA, in cooperazione con la Commissione e grazie al sostegno dell'ECCG e del suo pertinente sottogruppo per il mantenimento, garantisce il mantenimento dei sistemi europei di certificazione della cibersecurity, anche in considerazione di un'eventuale revisione di tali sistemi da parte della Commissione. L'ENISA coopera e scambia informazioni con i soggetti e i gruppi pertinenti dell'Unione in relazione alle attività di mantenimento. 5. L'ECCG può formulare un parere sul mantenimento dei sistemi europei di certificazione della cibersecurity.	Commissione europea ENISA ECCG Organismi di valutazione della conformità	L'ENISA garantisce il mantenimento, anche attraverso riunioni periodiche ibride o online, la raccolta di informazioni, l'analisi e la condivisione (in relazione a un sistema europeo di certificazione della cibersecurity)	Trattamento dei dati Flusso di dati
Articolo 76 Valutazione, revisione e ritiro di un sistema europeo di certificazione della cibersecurity	1. Almeno ogni quattro anni dopo l'entrata in applicazione di un sistema europeo di certificazione della cibersecurity l'ENISA valuta l'impatto e l'efficacia di tale sistema, in cooperazione con il pertinente sottogruppo dell'ECCG per il mantenimento e tenendo conto dei riscontri ricevuti dai portatori di interessi. L'ENISA effettua la valutazione attraverso un'analisi di mercato conformemente all'articolo 8, paragrafo 1. 3. In sede di revisione o di ritiro di sistemi europei di certificazione della cibersecurity, la Commissione consulta l'ENISA, l'ECCG e il relativo sottogruppo sul mantenimento e tiene altresì conto delle opinioni dei pertinenti portatori di interessi e di altri soggetti dell'Unione. 4. L'ECCG può formulare un parere sulla revisione o sul ritiro di un sistema europeo di certificazione della cibersecurity. La	Commissione europea ENISA ECCG	La Commissione rivede i sistemi consultando i portatori di interessi.	Trattamento dei dati Flusso di dati

	Commissione ne tiene debitamente conto in sede di revisione o di ritiro del sistema europeo di certificazione della cibersecurity.			
Articolo 77 Specifiche tecniche nei sistemi europei di certificazione della cibersecurity	3. Qualora siano richiamate in un sistema europeo di certificazione della cibersecurity, come previsto all'articolo 74, paragrafo 10, le specifiche tecniche sono rese disponibili sul sito web di cui all'articolo 79. 4. In casi debitamente giustificati, in particolare se le specifiche tecniche contengono informazioni che potrebbero compromettere la sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti certificati o la postura di cibersecurity dei soggetti, tali specifiche sono distribuite solo ai portatori di interessi cui si applicano i requisiti del sistema. Tale sistema non è richiamato in un sistema europeo di certificazione della cibersecurity di cui all'articolo 74, paragrafo 10.	ENISA Stati membri Organismi di valutazione della conformità	Messa a disposizione delle informazioni sul sito web dell'ENISA relativo alla certificazione	Flusso di dati Servizio pubblico digitale
Articolo 79 Sito web sui sistemi europei di certificazione della cibersecurity	1. L'ENISA organizza attività volte a promuovere la diffusione dei sistemi europei di certificazione della cibersecurity adottati, anche gestendo il sito web di cui al paragrafo 2 del presente articolo. 2. L'ENISA gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni pubbliche riguardanti: a) i sistemi europei di certificazione della cibersecurity;	ENISA Stati membri Organismi di valutazione della conformità	La gestione del sito web informativo impone all'ENISA di raccogliere, trattare e mantenere banche dati complete contenenti informazioni sulla certificazione, il che richiede attività di gestione dei dati su base continuativa.	Servizio pubblico digitale Soluzione digitale Trattamento dei dati Flusso di dati

	b) i diritti associati al mantenimento di ciascun sistema europeo di certificazione della cibersecurity; c) le pertinenti specifiche tecniche dell'ENISA; d) i certificati europei di cibersecurity e le dichiarazioni UE di conformità, comprese informazioni sui certificati e sulle dichiarazioni che non sono più validi o che sono sospesi, revocati o scaduti; e) le informazioni supplementari sulla cibersecurity pertinenti in conformità dell'articolo 84, paragrafo 2; f) le sintesi delle revisioni tra pari a norma dell'articolo 89, paragrafo 7; g) le specifiche tecniche richiamate in un sistema europeo di certificazione della cibersecurity a norma dell'articolo 74, paragrafo 10. 3. Ove applicabile, il sito web di cui al paragrafo 2 indica inoltre i sistemi di certificazione della cibersecurity nazionali che sono stati sostituiti da un sistema europeo di certificazione della cibersecurity.			
Articolo 81 Elementi del sistema europeo di certificazione della cibersecurity	5. Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscano principi comuni e disposizioni tipo per gli elementi di cui ai paragrafi 1, 2 e 3 in tutti i sistemi europei di certificazione della cibersecurity. Un sistema europeo di certificazione della cibersecurity può includere riferimenti a tali principi e disposizioni tipo, se del caso e ove disponibili. Gli atti di esecuzione di cui al paragrafo 5 sono	ENISA Pubblico in generale Autorità degli Stati membri	Consultazione dei pertinenti portatori di interessi che richiede flussi di dati e operazioni di trattamento dei dati	Flusso di dati Trattamento dei dati

	adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2. Nell'elaborare o rivedere i principi comuni e le disposizioni tipo per gli elementi dei sistemi europei di certificazione della cibersecurity, la Commissione consulta l'ENISA e tiene conto, se del caso, delle opinioni dell'ECCG, dei pertinenti portatori di interessi e di altri organismi pertinenti.			
Articolo 83 Autovalutazione della conformità	3. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti o il soggetto la cui postura di cibersecurity è oggetto di certificazione rende disponibile all'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 89, per il periodo stabilito nel sistema europeo di certificazione della cibersecurity, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità al sistema dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o della postura di cibersecurity. Una copia della dichiarazione UE di conformità è trasmessa senza indebito ritardo all'autorità nazionale di certificazione della cibersecurity e all'ENISA.	ENISA Pubblico in generale Autorità degli Stati membri	Disponibilità delle informazioni; condivisione dei dati I dati condivisi devono essere oggetto di trattamento da parte dell'ENISA e delle autorità degli Stati membri	Flusso di dati Trattamento dei dati
Articolo 84 Informazioni supplementari sulla cibersecurity dei prodotti TIC, servizi TIC e processi TIC certificati	1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC per i quali è stata rilasciata una dichiarazione UE di conformità o è stato rilasciato un certificato europeo di cibersecurity rende pubblicamente	Fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC Pubblico in generale Organismi di valutazione della	Rendere pubblicamente disponibili le informazioni in formato elettronico.	Flusso di dati

	disponibili le seguenti informazioni supplementari sulla cibersecurity.	conformità		
Articolo 85 Rilascio di certificati europei di cibersecurity	2. Gli organismi di valutazione della conformità di cui all'articolo 91 rilasciano certificati europei di cibersecurity sulla base dei criteri previsti dal sistema europeo di certificazione della cibersecurity adottato a norma dell'articolo 74. 6. La persona fisica o giuridica che presenta i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per la certificazione o il soggetto che richiede la certificazione della propria postura di cibersecurity mette a disposizione dell'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 89, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersecurity, o dell'organismo di valutazione della conformità di cui all'articolo 91 tutte le informazioni necessarie a espletare la certificazione. 7. Gli organismi di valutazione della conformità e, se del caso, le autorità nazionali di certificazione della cibersecurity informano l'ENISA senza indebito ritardo in merito alle loro decisioni che incidono sullo stato dei certificati europei di cibersecurity e delle dichiarazioni UE di conformità a norma dell'articolo 94. 8. Il titolare di un certificato europeo di cibersecurity informa l'organismo di valutazione della conformità e, se del caso, l'autorità nazionale di certificazione della cibersecurity di cui al paragrafo 7 delle eventuali vulnerabilità o non conformità	ENISA Pubblico in generale Autorità degli Stati membri Organismi di valutazione della conformità	Condivisione di informazioni pertinenti ai processi di certificazione	Flusso di dati Trattamento dei dati

	successivamente rilevate, in relazione al prodotto TIC, al servizio TIC, al processo TIC o al servizio di sicurezza gestito certificato o alla postura di cibersecurity del soggetto certificata, che hanno la probabilità di incidere sulla conformità al certificato. Tale organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersecurity interessata e valuta l'impatto sul certificato in linea con le condizioni del sistema indicate all'articolo 81, lettera f).			
Articolo 86 Sistemi nazionali di certificazione della cibersecurity	4. Gli Stati membri informano la Commissione e l'ECCG prima di adottare nuovi sistemi nazionali di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti e la postura di cibersecurity dei soggetti.	ENISA Stati membri Commissione europea	Condivisione delle informazioni	Flusso di dati
Articolo 88 Autorità nazionali di certificazione della cibersecurity	2. Ciascuno Stato membro comunica alla Commissione l'identità delle autorità nazionali di certificazione della cibersecurity designate. Se uno Stato membro designa più di una autorità, comunica alla Commissione anche i compiti assegnati a ciascuna di tali autorità. 6. Le autorità nazionali di certificazione della cibersecurity: c) controllano, in cooperazione con le autorità di vigilanza del mercato competenti, la conformità agli obblighi che, ai sensi del presente regolamento, incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o ai soggetti la cui postura di cibersecurity è certificata che sono stabiliti nei	ENISA Autorità degli Stati membri Commissione europea Pubblico in generale Organismi di valutazione della conformità	Gli Stati membri comunicano alla Commissione le autorità nazionali di certificazione della cibersecurity designate. Le autorità degli Stati membri svolgono vari compiti di monitoraggio, supervisione e cooperazione che richiedono flussi di dati e operazioni di trattamento dei dati	Flusso di dati Trattamento dei dati

	rispettivi territori e che effettuano un'autovalutazione della conformità nel corrispondente sistema europeo di certificazione della ciphersicurezza e fanno applicare tali obblighi; d) fatto salvo l'articolo 91, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento o altre autorità pertinenti nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento; e) cooperano con la Commissione qualora la competenza di un organismo di valutazione della conformità sia contestata a norma dell'articolo 94; f) vigilano sulle attività degli organismi pubblici di cui all'articolo 85, paragrafo 3, e le monitorano; g) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 93, controllano la conformità ai requisiti specifici o supplementari stabiliti nei sistemi europei di certificazione della ciphersicurezza a norma dell'articolo 81, paragrafo 3, lettera f), e fanno applicare gli obblighi che incombono agli organismi di valutazione della conformità in relazione a tali requisiti e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità non si conformino alle prescrizioni del presente regolamento; h) trattano i reclami delle persone fisiche			
--	---	--	--	--

	o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità ai sensi dell'[articolo 85, paragrafo 4], oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 83, e svolgono le indagini opportune sull'oggetto di tali reclami e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole; i) trasmettono alla Commissione, all'ENISA e all'ECCG una relazione annuale sulle loro principali attività entro il 31 marzo di ogni anno a decorrere dal [anno di entrata in vigore + 12 mesi] e la mettono a disposizione del gruppo incaricato della revisione tra pari ove l'autorità nazionale di certificazione della cibersicurezza sia soggetta a una revisione tra pari a norma dell'articolo 89; j) cooperano con le altre autorità nazionali di certificazione della cibersicurezza, con le autorità di vigilanza del mercato o con altre autorità pubbliche, anche mediante lo scambio di informazioni sull'eventuale non conformità dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti e della postura di cibersicurezza dei soggetti ai requisiti del presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza; k) monitorano gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza.			
--	---	--	--	--

	8. Le autorità nazionali di certificazione della cibersecurity cooperano tra di loro e con la Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersecurity e le questioni tecniche riguardanti la cibersecurity dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti e la postura di cibersecurity dei soggetti. 9. Entro il [entrata in vigore + 6 mesi] l'ENISA elabora un modello per la relazione di cui al paragrafo 6, lettera i), del presente articolo, in cooperazione con la Commissione e l'ECCG.			
Articolo 89 Revisione tra pari	5. L'ENISA sostiene l'organizzazione del meccanismo di revisione tra pari e delle revisioni stesse, anche elaborando documenti di orientamento e modelli pertinenti, in cooperazione con la Commissione e l'ECCG. 7. La relazione finale, compresi eventuali orientamenti o raccomandazioni, e la sintesi della revisione tra pari sono esaminate dall'ECCG, che approva la sintesi per la pubblicazione sul sito web di cui all'articolo 79, paragrafo 2.	UE ENISA ECCG	Messa a disposizione online dei dati	Flusso di dati Trattamento dei dati
Articolo 90 Gruppo europeo per la certificazione della cibersecurity (ECCG)	3. L'ECCG ha i seguenti compiti: [riferimento ad altri articoli] h) esaminare gli sviluppi pertinenti al settore della certificazione della cibersecurity, anche a livello nazionale ai sensi dell'articolo 86, e scambiare informazioni e buone pratiche sui sistemi europei di certificazione della	Stati membri ENISA Commissione europea	Analisi, condivisione di informazioni e cooperazione tra le autorità degli Stati membri e le organizzazioni internazionali in relazione alla certificazione europea della cibersecurity	Trattamento dei dati Flusso di dati

	cibersicurezza; i) agevolare la cooperazione tra le autorità nazionali di certificazione della cibersicurezza secondo le prescrizioni del presente titolo attraverso lo sviluppo di capacità e lo scambio di informazioni, in particolare in relazione agli aspetti della certificazione della cibersicurezza; [riferimento ad altri articoli] k) agevolare l'allineamento dei sistemi europei di certificazione della cibersicurezza alle norme riconosciute a livello internazionale, anche nell'ambito del mantenimento dei sistemi europei di certificazione della cibersicurezza esistenti e, ove opportuno, rivolgere raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni di normazione europee o internazionali per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello europeo o internazionale.			
Articolo 92 Ulteriore armonizzazione della competenza degli organismi di valutazione della conformità	4. Qualora riceva una richiesta ai sensi del paragrafo 3, un'autorità nazionale di certificazione della cibersicurezza ne informa l'autorità nazionale di certificazione della cibersicurezza dello Stato membro in cui è stabilito il richiedente organismo di valutazione della conformità. In tali casi l'autorità nazionale di certificazione della cibersicurezza di tale Stato membro può partecipare al processo di autorizzazione in qualità di osservatore.	Autorità degli Stati membri Organismi di valutazione della conformità	Condivisione e conservazione delle informazioni	Flusso di dati Trattamento dei dati
Articolo 93 Notifiche degli organismi di	1. Per ciascun sistema europeo di certificazione della cibersicurezza le autorità nazionali di	ENISA Stati membri	Notifiche degli organismi di valutazione della conformità	Flussi di dati Trattamento

valutazione della conformità	certificazione della cibersecurity di uno Stato membro notificano alla Commissione e agli altri Stati membri gli organismi di valutazione della conformità che sono stati accreditati e, se del caso, autorizzati a norma dell'articolo 92. 2. Le autorità nazionali di certificazione della cibersecurity effettuano la notifica di cui al paragrafo 1 utilizzando lo strumento elettronico di notifica sviluppato e gestito dalla Commissione.	Commissione europea Organismi di valutazione della conformità	accreditati e autorizzati	dei dati
Articolo 94 Contestazione della competenza degli organismi di valutazione della conformità	1. 1. La Commissione indaga sui casi in cui abbia dubbi o venga a conoscenza di dubbi sulla competenza di un organismo di valutazione della conformità ad adempiere le prescrizioni e le responsabilità che ad esso incombono, o sul continuo adempimento, da parte di tale organismo, di tali prescrizioni e responsabilità. 2. L'autorità nazionale di certificazione della cibersecurity fornisce alla Commissione , su richiesta, tutte le informazioni relative alla base della notifica o del mantenimento della competenza dell'organismo di valutazione della conformità in questione. 3. La Commissione garantisce la riservatezza di tutte le informazioni sensibili raccolte nel corso delle sue indagini. 4. La Commissione, qualora accerti che un organismo di valutazione della conformità non soddisfa o non soddisfa più i requisiti per la sua notifica, ne informa l'autorità nazionale di certificazione della cibersecurity e chiede a quest'ultima di adottare le misure correttive necessarie, incluso all'occorrenza il ritiro della	Commissione Stati membri ENISA	Contestazione della competenza degli organismi di valutazione della conformità	Flusso di dati Trattamento dei dati Servizio pubblico digitale

	notifica.			
Articolo 95 Obbligo di informazione e conservazione a carico degli organismi di valutazione della conformità	1. Gli organismi di valutazione della conformità informano l'autorità nazionale di certificazione della cibersecurity: a) di qualunque rifiuto, limitazione, sospensione o ritiro di un certificato; b) di qualunque circostanza che influisca sull'ambito e sulle condizioni della notifica di cui all'articolo 93, paragrafo 1; c) di qualunque richiesta di informazioni che abbiano ricevuto dalle autorità di vigilanza del mercato in relazione ad attività di valutazione della conformità; d) su richiesta, delle attività di valutazione della conformità eseguite nell'ambito della loro notifica e di qualsiasi altra attività svolta, incluse quelle transfrontaliere e di subappalto. 2. Gli organismi di valutazione della conformità forniscono inoltre all'ENISA le informazioni di cui al paragrafo 1, lettera a), al fine di agevolare lo svolgimento dei suoi compiti a norma dell'articolo 79. 3. Gli organismi di valutazione della conformità forniscono senza indebito ritardo agli altri organismi di valutazione della conformità a norma del presente regolamento, le cui attività di valutazione della conformità sono simili e hanno come oggetto gli stessi prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o soggetti la cui postura di cibersecurity è oggetto di certificazione, informazioni	Autorità degli Stati membri Organismi di valutazione della conformità	Scambio di informazioni da parte degli organismi di valutazione della conformità	Flusso di dati Trattamento dei dati

	pertinenti su questioni relative ai risultati negativi e, su richiesta, ai risultati positivi delle valutazioni della conformità. 4. Gli organismi di valutazione della conformità mantengono un sistema di registri in cui sono contenuti tutti i documenti e le prove presentati o ricevuti in relazione a ciascuna valutazione e certificazione da essi effettuata. I registri sono conservati in modo sicuro e accessibile per il periodo necessario ai fini della certificazione e per almeno cinque anni dopo la scadenza o la revoca di un certificato europeo di cibersecurity pertinente.			
Articolo 96 Diritto di presentare un reclamo e diritto a un ricorso giurisdizionale effettivo	2. L'autorità o l'organismo a cui è stato presentato il reclamo informa il reclamante dello stato del procedimento, della decisione adottata e del diritto a un ricorso giurisdizionale effettivo di cui ai paragrafi 3 e 4. 4. I procedimenti a norma del presente articolo sono presentati dinanzi ai tribunali dello Stato membro in cui ha sede l'autorità o l'organismo contro cui è mosso il ricorso giurisdizionale.	Autorità degli Stati membri Commissione europea Pubblico in generale Titolari di certificati	Flusso di informazioni tra le autorità e il pubblico in generale in merito ai reclami Procedimenti dinanzi ai tribunali dello Stato membro	Flusso di dati
Articolo 97 Sanzioni	Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.	Autorità degli Stati membri Commissione europea	Flusso di informazioni relative alla notifica delle sanzioni da parte degli Stati membri alla Commissione.	Flusso di dati

Articolo 99 Valutazioni dei rischi per la sicurezza	La Commissione o almeno tre Stati membri possono chiedere al gruppo di cooperazione NIS di effettuare valutazioni coordinate dei rischi entro sei mesi. La Commissione può chiedere termini più brevi. Le valutazioni dei rischi elaborano scenari di rischio e presuppongono un'analisi dei dati. Preparazione delle valutazioni coordinate dei rischi per la sicurezza Nei casi che giustificano un intervento immediato, la Commissione consulta senza ritardo gli Stati membri ed effettua una valutazione dei rischi. Decisioni per intraprendere valutazioni dei rischi (elaborazione/analisi dei dati).	Commissione europea Stati membri dell'UE Gruppo di cooperazione NIS ENISA	Richiesta e ricezione di informazioni; analisi dei dati ai fini delle valutazioni coordinate dei rischi Consultazione con gli Stati membri ed esecuzione di una valutazione dei rischi	Trattamento dei dati Flusso di dati
Articolo 100, paragrafi 1 e 2 Designazione dei paesi terzi che destano preoccupazioni per la cibersicurezza	1. Qualora, a seguito della valutazione dei rischi per la sicurezza di cui all'articolo 99 o sulla base di altre fonti, come una dichiarazione pubblica a nome dell'Unione o di uno Stato membro, risulti che un paese terzo presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione verifica la minaccia rappresentata da tale paese, tenendo conto di una serie di elementi che porteranno al trattamento/all'analisi dei dati. 2. Qualora, a seguito della verifica di cui al paragrafo 1, concluda che un paese terzo	Stati membri dell'UE Commissione europea	Ricezione, analisi e scambio di informazioni.	Flussi di dati Trattamento dei dati

	presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la Commissione può decidere, mediante un atto di esecuzione, di designare tale paese terzo come paese che desta preoccupazioni per la cibersicurezza per le catene di approvvigionamento delle TIC, con conseguente analisi/trattamento dei dati e flussi di dati.			
Articolo 101 Meccanismo generale riguardante le catene di approvvigionamento delle TIC Articolo 102 Individuazione delle risorse TIC chiave	1. Qualora il gruppo di cooperazione NIS abbia effettuato una valutazione coordinata dei rischi per la sicurezza a livello dell'Unione a norma dell'articolo 99, paragrafi 1 e 2, del presente regolamento, o dopo il completamento della procedura in caso di minaccia informatica significativa a norma dell'articolo 99, paragrafo 3, la Commissione può adottare le misure di cui agli articoli 102 e 103. Alla Commissione è conferito il potere di adottare atti di esecuzione che definiranno le risorse TIC chiave e le misure di attenuazione, nonché le restrizioni e i divieti riguardanti le catene di approvvigionamento delle TIC (descritti in dettaglio nella sezione 4.5). In preparazione di tale processo, la Commissione tiene conto di diversi aspetti che evocano il trattamento/l'analisi dei	Commissione europea Gruppo di cooperazione NIS Portatori di interessi pertinenti	Analisi dei dati/trattamento dei dati; consultazione dei portatori di interessi pertinenti	Trattamento dei dati Flusso di dati

Articolo 103 Misure di attenuazione nelle catene di approvvigionamento delle TIC	dati e, in alcuni casi, il flusso dei dati: Articolo 102, lettere da a) a f) Articolo 103, paragrafo 4, lettere da a) a d) Articolo 103, paragrafo 6			
Articolo 104 Individuazione dei fornitori ad alto rischio	Mediante atti di esecuzione, la Commissione stila elenchi di fornitori ad alto rischio pertinenti ai fini dei divieti stabiliti negli atti di esecuzione adottati a norma dell'articolo 103, paragrafo 1, o del divieto di cui all'articolo 111, paragrafo 1. La Commissione effettua una mappatura dei fornitori di componenti TIC e di componenti che comprendono componenti TIC e conduce una valutazione iniziale per individuare quali dei fornitori sono potenzialmente stabiliti in paesi terzi o controllati da tali paesi terzi designati a norma dell'articolo 100. La Commissione valuta il luogo di stabilimento nonché l'assetto proprietario e di controllo. La Commissione ha la facoltà di richiedere ai fornitori le informazioni necessarie, condivide con i fornitori interessati le conclusioni preliminari relative alla valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo e	Commissione europea Autorità competenti Fornitori	Analisi dei dati/trattamento dei dati; consultazione delle autorità competenti, consultazione dei fornitori	Trattamento dei dati Flusso di dati

	concede loro la possibilità di essere ascoltati. La Commissione può chiedere a un'autorità competente di effettuare la valutazione iniziale del luogo di stabilimento e dell'assetto proprietario e di controllo di un fornitore, ove giustificato alla luce delle caratteristiche dell'attività di tale fornitore. Un'autorità competente può offrirsi di effettuare tale valutazione iniziale. La Commissione verifica tali conclusioni iniziali al fine di decidere se il fornitore debba essere incluso nell'elenco dei fornitori ad alto rischio. La Commissione aggiorna regolarmente gli elenchi dei fornitori ad alto rischio al fine di eliminare o aggiungere fornitori ad alto rischio. I fornitori ad alto rischio inclusi nell'elenco possono chiedere alla Commissione di effettuare una nuova valutazione del loro luogo di stabilimento e del loro assetto proprietario e di controllo, dietro presentazione di elementi attestanti i cambiamenti intervenuti a tale riguardo.			
--	---	--	--	--

Articolo 105 Esenzione dei soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersicurezza o controllati da soggetti di tale paese terzo Articolo 108 Riservatezza	1. Un soggetto stabilito in un paese terzo designato che desta preoccupazioni per la cibersicurezza oppure controllato da tale paese terzo può presentare una richiesta motivata alla Commissione. 3. La Commissione valuta e adotta una decisione tenendo conto di diversi aspetti che conducono all'analisi dei dati. (Articolo 105, paragrafi 3 e 4) Le informazioni ricevute dalla Commissione sono utilizzate soltanto per la finalità per la quale sono state acquisite.	Commissione europea Soggetti stabiliti in un paese terzo designato che desta preoccupazioni per la cibersicurezza o controllati da soggetti di tale paese terzo	La Commissione riceve la richiesta e analizza i dati.	Flusso di dati Trattamento dei dati
Articolo 107 Registro	La Commissione tiene un registro accessibile al pubblico delle decisioni adottate a norma dell'articolo 105. Il registro riporta i nomi dei soggetti destinatari delle decisioni.	Commissione europea Soggetti stabiliti in un paese terzo designato che desta preoccupazioni per la cibersicurezza o controllati da tale paese terzo	La Commissione tiene un registro accessibile al pubblico.	Soluzione digitale
Articolo 111 Divieti per le reti di comunicazione elettronica mobili, fisse e satellitari	L'autorità competente designata a norma del presente regolamento informa senza ritardo l'autorità competente a norma del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali] in merito alle misure imposte ai fornitori di reti di comunicazione elettronica mobili, fisse e satellitari.	Autorità competente ai sensi dell'articolo 9 o dell'articolo 20 del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali] Fornitori di reti di comunicazione elettronica mobili, fisse e satellitari	Informazioni inviate dall'autorità competente ai soggetti in relazione alle autorizzazioni.	Flusso di dati

Articolo 112, paragrafi 1 e 4 Autorità competenti	1. Ciascuno Stato membro designa una o più autorità competenti responsabili dei compiti di vigilanza e di esecuzione di cui all'articolo 114. 4. Ciascuno Stato membro notifica senza indebito ritardo alla Commissione i nomi delle autorità competenti designate a norma del paragrafo 1, i compiti rispettivi di tali autorità e qualsiasi successiva modifica degli stessi. Ciascuno Stato membro rende inoltre pubblici i nomi delle autorità competenti designate a norma del paragrafo 1.	Stati membri dell'UE Commissione europea Pubblico in generale	Gli Stati membri designano le autorità competenti e ne danno notifica alla Commissione.	Flusso di dati
Articolo 113 Rete dei servizi di cooperazione e di sostegno della Commissione	1. La Commissione istituisce una rete di cooperazione tra le autorità competenti degli Stati membri e la Commissione, che funga da piattaforma per la cooperazione e lo scambio di informazioni. La Commissione fornisce alla rete sostegno amministrativo. 2. Al fine di sostenere gli Stati membri nell'esecuzione dei loro compiti di vigilanza, la Commissione valuta se i fornitori che potrebbero essere interessati da divieti specifici sono stabiliti in paesi terzi che desta preoccupazioni per la cibersecurity, designati a norma dell'articolo 100, o controllati da tali paesi. A tal fine, l'autorità competente condivide le informazioni	Commissione Autorità competenti Soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555	Valutazione da parte della Commissione dei fornitori e condivisione delle conclusioni con le autorità competenti, che condividono a loro volta tali informazioni con i soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555 La Commissione richiede informazioni ai fornitori Autorità competenti che informano la Commissione	Trattamento dei dati Flussi di dati

	pertinenti con la Commissione. 3. Ai fini della valutazione, la Commissione ha la facoltà di richiedere le informazioni necessarie ai fornitori che potrebbero essere interessati da divieti specifici e che sono stabiliti in paesi terzi designati a norma dell'articolo 100 o controllati da tali paesi terzi. 4. Una volta completato il processo di valutazione, la Commissione condivide le proprie conclusioni con le autorità competenti nell'ambito della rete istituita a norma del paragrafo 1. Le autorità competenti condividono a tempo debito tali conclusioni con i soggetti interessati del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555. 5. Qualora un'autorità competente venga a conoscenza del fatto che un fornitore che potrebbe essere interessato da divieti specifici è stabilito in paesi terzi che desta preoccupazioni per la cibersecurity o controllato da tali paesi e non è stato sottoposto ad alcuna valutazione, ne informa senza indebito ritardo la Commissione.			
--	---	--	--	--

Articolo 114 Misure di vigilanza e di esecuzione	Obbligo per gli Stati membri di garantire la condivisione di informazioni con i soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555. Prima di adottare le misure le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Le autorità competenti cooperano tra di loro e con la Commissione.	Stati membri dell'UE Commissione europea Soggetti nel contesto degli allegati I e II della direttiva (UE) 2022/2555	Prescrizioni volte a garantire un flusso di informazioni	Flusso di dati Trattamento dei dati
Articolo 115 Sanzioni	Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.	Commissione europea Stati membri dell'UE	Notifica alla Commissione da parte degli Stati membri	Flusso di dati
Articolo 116 Assistenza reciproca	Se un soggetto di cui all'allegato I o II della direttiva (UE) 2022/2555 fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e le sue risorse chiave sono ubicate in uno o più Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità. L'assistenza reciproca di cui al primo comma. Lettera c), può riguardare richieste di informazioni e misure di vigilanza,	Stati membri dell'UE	Assistenza reciproca nel quadro di attività di vigilanza.	Flusso di dati Trattamento dei dati

	comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza congiunte.			
--	--	--	--	--

Articolo 1, punto 8), della direttiva Segnalazione di attacchi ransomware (Articolo 27, paragrafo 13, NIS2)	all'articolo 23 sono aggiunti i paragrafi 12 e 13 seguenti: "13. Gli Stati membri provvedono affinché, in caso di incidente significativo causato da un attacco ransomware, i soggetti interessati informino, su richiesta del CSIRT o, se del caso, l'autorità competente attraverso un canale di comunicazione fornito dal CSIRT o, se del caso, l'autorità competente: se il soggetto ha ricevuto una richiesta di riscatto e, se del caso, da chi; se è stato pagato un riscatto; in caso affermativo è necessario comunicare l'importo, i mezzi di pagamento e il destinatario finale, tra cui il fornitore di cripto-attività e il fornitore di servizi per le cripto-attività, se del caso."	Stati membri dell'UE Soggetti essenziali e importanti	Segnalazione	Flusso di dati
Articolo 1, punto 10), della direttiva Elenco dei soggetti e registro (Articolo 27, paragrafo 1, NIS2)	L'ENISA crea e mantiene un registro dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 2.	ENISA Stati membri dell'UE (soggetti essenziali e importanti ai sensi della direttiva NIS 2, soggetti che forniscono servizi di registrazione dei nomi di dominio)	L'ENISA crea e mantiene un registro	Soluzione digitale Servizio pubblico digitale
Articolo 1, punto 11), della direttiva Elenco dei soggetti e registro (Articolo 27, paragrafo 4, NIS2)	"4. In seguito alla ricezione delle informazioni di cui all'articolo 3, paragrafo 4, il punto di contatto unico dello Stato membro interessato, senza ritardo, le inoltra all'ENISA."	ENISA Stati membri dell'UE	Condivisione delle informazioni da parte degli Stati membri con l'ENISA	Flusso di dati
Articolo 1, punto 12), della direttiva	1. L'ENISA assiste gli Stati membri nel quadro dell'assistenza reciproca ai sensi	ENISA Stati membri dell'UE	L'ENISA assiste gli Stati membri e contribuisce ad agevolare il	Trattamento dei dati

Assistenza reciproca (Articolo 37 bis, paragrafi 1, 2 e 3, NIS 2)	dell'articolo 37 e contribuisce ad agevolare tali processi di cooperazione per i soggetti essenziali e importanti (...). 2. L'ENISA effettua un'analisi completa (...). L'ENISA, in collaborazione con la Commissione e il gruppo di cooperazione, elabora una metodologia. La relazione è aggiornata annualmente. "3. L'ENISA, se del caso, formula raccomandazioni, elabora orientamenti, fornisce assistenza (...)	Soggetti importanti ed essenziali ai sensi della direttiva NIS 2 Commissione europea	processo di cooperazione. Svolge analisi, formula orientamenti e metodologie, e redige relazioni.	Flusso di dati
Articolo 1, punto 12), della direttiva Assistenza reciproca (Articolo 37 bis, paragrafo 4, NIS 2)	4. Ai fini del paragrafo 4, lettera e), del presente articolo, le autorità competenti degli Stati membri interessati forniscono all'ENISA, se disponibili, quanto segue (...). 5. Qualora uno Stato membro riceva assistenza, conformemente a quanto previsto all'articolo 37, paragrafo 1, primo comma, lettera c), il punto di contatto unico informa l'ENISA che vi è stata assistenza reciproca.	ENISA Stati membri dell'UE	Scambio di informazioni	Flusso di dati
Articolo 119 Esercizio della delega	3. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.	Commissione europea Parlamento europeo Consiglio	Informazioni trasmesse al PE e al Consiglio	Flusso di dati
Articolo 120 Valutazione e riesame	1. Entro il [GG MM AAAA] e, successivamente, ogni cinque anni la Commissione commissiona una valutazione dei risultati conseguiti dall'ENISA in relazione agli obiettivi, al mandato, alla missione, ai compiti, alla governance e all'ubicazione della stessa, conformemente agli orientamenti della Commissione. 5. La Commissione riferisce al Parlamento europeo, al Consiglio e al consiglio di amministrazione sui risultati della valutazione. Il	ENISA Commissione Pubblico in generale	Raccolta e analisi dei dati; rendere pubbliche le informazioni disponibili	Trattamento dei dati Flusso di dati

	risultati della valutazione sono resi pubblici.			
--	---	--	--	--

4.2. Dati

Descrizione di alto livello dei dati nell'ambito di applicazione e di qualsiasi norma/specifica correlata

Tipo di dati	Riferimento alle prescrizioni	Norma e/o specifica (se del caso)
Dati connessi ad analisi/relazioni pertinenti alla ciberresilienza della società	Articolo 5, paragrafo 1, lettere a), b), c), e), f), h) Articolo 5, paragrafi 2, 3 e 4 Articolo 6 Articolo 7 Articolo 8 Articolo 9 Articolo 10 Articolo 11, paragrafo 2, lettere b) e c) Articolo 12, paragrafo 4 Articolo 15 Articolo 1, punto 7), della direttiva	Nel quadro delle attività elencate all'articolo 11, paragrafo 1, lettere da a) a e), e all'articolo 11, paragrafo 2, l'ENISA utilizza le proprie analisi e, se del caso, le informazioni ricevute nello svolgimento dei suoi compiti, tra cui: a) le informazioni fornite tramite fonti accessibili al pubblico, comprese le vulnerabilità pubblicamente note riguardanti i prodotti TIC o i servizi TIC disponibili nella banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555; b) le informazioni condivise da Stati membri, da soggetti dell'Unione, dal CERT-UE, da partner del settore privato o non governativi nonché da paesi terzi e organizzazioni internazionali, fatte salve eventuali limitazioni all'ulteriore distribuzione di tali informazioni mediante un contrassegno visibile. L'ENISA emana orientamenti relativi all'interoperabilità dei sistemi informativi di rete utilizzati per la condivisione delle informazioni, anche per quanto riguarda i poli informatici

		transfrontalieri di cui all'articolo 6, paragrafo 3, del regolamento (UE) 2025/38.
Dati pertinenti alla cooperazione operativa e alla conoscenza situazionale	Articolo 10, paragrafo 4, lettere da a) a g) Articolo 10, paragrafo 6 Articolo 11, paragrafo 1, lettere da a) a g) Articolo 11, paragrafo 2, lettere a), b) e c) Articolo 11, paragrafo 3 Articolo 11, paragrafo 4 Articolo 13, paragrafo 2 Articolo 15 Articolo 16, paragrafo 2, lettera e)	Norme in materia di riservatezza e trattamento delle informazioni sensibili Nel quadro delle attività elencate all'articolo 11, paragrafo 1, lettere da a) a e), e all'articolo 11, paragrafo 2, l'ENISA utilizza le proprie analisi e, se del caso, le informazioni ricevute nello svolgimento dei suoi compiti, tra cui: a) le informazioni fornite tramite fonti accessibili al pubblico, comprese le vulnerabilità pubblicamente note riguardanti i prodotti TIC o i servizi TIC disponibili nella banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555; b) le informazioni condivise da Stati membri, da soggetti dell'Unione, dal CERT-UE, da partner del settore privato o non governativi nonché da paesi terzi e organizzazioni internazionali, fatte salve eventuali limitazioni all'ulteriore distribuzione di tali informazioni mediante un contrassegno visibile.
Dati pertinenti ai sistemi europei di attestazione delle competenze individuali in materia di cibersecurity e all'autorizzazione dei fornitori Dati pertinenti agli obiettivi, alle finalità e al contenuto dei sistemi europei di certificazione della cibersecurity	Articolo 17 Articolo 18 Articoli da 19 a 23 Articoli 72, 73, 74, 75, 76, 77, 79, 81, 83, 84	Un sistema europeo di attestazione delle competenze individuali in materia di cibersecurity comprende (...): le norme relative alla conservazione dei registri da parte dei fornitori autorizzati di attestati I soggetti autorizzati garantiscono che, su richiesta dell'interessato, gli attestati europei delle competenze individuali in materia di cibersecurity siano rilasciati sotto forma di attestati elettronici di attributi in un formato che può essere archiviato nei portafogli europei di identità digitale di cui al regolamento (UE) n. 910/2014. La Commissione e l'ENISA dovrebbero seguire le pertinenti

		disposizioni della legislazione dell'Unione quando si tratta di istituire un sistema europeo di certificazione della cibersecurity per quanto riguarda i dati.
Dati relativi alla governance del quadro europeo di certificazione della cibersecurity	Articoli 85, 86, 88, 89, 90, 92, 93, 94, 95, 96, 97	L'ENISA, gli organismi di valutazione della conformità e le autorità nazionali di certificazione della cibersecurity dovrebbero garantire la riservatezza dei dati e seguire le disposizioni di un regime pertinente che faccia riferimento a norme internazionali che specifichino le prescrizioni da rispettare.
Dati pertinenti alle funzioni interne dell'ENISA (bilancio, DOCUP, strategie interne)	Articolo 25 Articolo 28, paragrafo 1 Articolo 30 Articolo 31, paragrafo 8 Articolo 32, paragrafi 3 e 5 Articolo 35, paragrafi 5 e 6 Articoli da 36 a 43 Articolo 44 Articolo 45 Articolo 47, paragrafo 10 Articoli 48 e 49 Articoli 52 e 58	Modelli e orientamenti riguardanti la regolamentazione finanziaria; orientamenti interni
Dati personali	Articolo 22 Titolo II, capo III, sezione 6 Commissione di ricorso Articolo 66 Articolo 80, paragrafo 1, lettere c) e x)	Regolamento (UE) 2018/1725 Regolamento (UE) 2016/679

	Articolo 81, paragrafo 2 Articolo 88, paragrafo 6, lettera h) Articolo 95 Articolo 96	
Dati raccolti e analizzati nel contesto dello svolgimento di valutazioni coordinate dei rischi, dell'elaborazione di scenari di rischio e dell'individuazione delle risorse TIC chiave	Articolo 98 Articolo 99 Articolo 102 Articolo 103 Articolo 105	Fatti salvi l'articolo 13 del regolamento (UE) 2024/2847 e l'articolo 21 della direttiva (UE) 2022/2555
Dati relativi a paesi terzi/soggetti di paesi terzi	Articolo 100, paragrafi 1, 3 e 4 Articolo 104 Articolo 105 Articolo 107 Articolo 113	N/D
Dati relativi alle autorità nazionali	Articolo 112 Articolo 114 Articolo 116	N/D
Dati pertinenti alle valutazioni dei rischi	Articolo 5, paragrafo 2	Norme in materia di riservatezza e trattamento delle informazioni sensibili
Assistenza reciproca tra Stati membri	Articolo 5, paragrafo 1, lettera g), del presente regolamento e articolo 1, punto 12), della direttiva	/

Allineamento con la strategia europea per i dati

Spiegare in che modo le prescrizioni sono allineate alla strategia europea per i dati

Le prescrizioni contenute nella proposta relativa al regolamento sulla cibersicurezza 2 sono allineate senza alcun impatto specifico sulla strategia europea per i dati.

Allineamento con il principio "una tantum"

Spiegare in che modo è stato preso in considerazione il principio "una tantum" ed è stata esaminata la possibilità di riutilizzare i dati esistenti

Uno degli obiettivi della proposta è massimizzare gli sforzi di semplificazione della Commissione e ridurre gli oneri amministrativi per gli Stati membri e i portatori di interessi. Negli ultimi anni l'ENISA è diventata un polo di informazione, presso il quale sono disponibili informazioni provenienti da diverse fonti. In tal senso, molti dei compiti dell'ENISA sono associati al riutilizzo e al riciclo delle informazioni per scopi legati a diverse analisi. Ad esempio: per determinati scopi, riutilizzo delle informazioni notificate a norma degli articoli 23 e 30 della direttiva (UE) 2022/2555, nonché delle informazioni notificate, condivise o analizzate a norma dell'articolo 14, paragrafi da 1 a 3, dell'articolo 15 e dell'articolo 17, paragrafi 1 e 3, del regolamento (UE) 2024/2847. Le disposizioni del quadro riguardante le catene di approvvigionamento presuppongono che la sua attuazione sia corroborata dai dati ricevuti a norma dell'articolo 22 della direttiva (UE) 2022/2555, il che dimostra la necessità del riutilizzo delle informazioni e delle attività di coordinamento.

Spiegare in che modo i nuovi dati sono reperibili, accessibili, interoperabili e riutilizzabili e soddisfano livelli di qualità elevati

La proposta legislativa indica esplicitamente quando i dati dovrebbero essere resi pubblici. Nell'ambito di tale proposta si sta valutando la natura delle disposizioni con aspetti strettamente legati alla sicurezza e alla riservatezza e pertanto non tutti i dati creati nel quadro del regolamento sulla cibersicurezza riveduto saranno destinati a essere resi pubblici. Per le disposizioni necessarie, è stato garantito l'allineamento al portafoglio europeo di identità digitale. L'ENISA ha il compito di proporre un servizio di allerta precoce in un formato leggibile tramite un dispositivo automatico.

Flussi di dati

Descrizione di alto livello dei dati nell'ambito di applicazione e di qualsiasi norma/specifica correlata

Tipo di dati	Spiegazione del flusso di dati	Riferimenti
L'ENISA fornisce relazioni e analisi, orientamenti tecnici e migliori pratiche.	Si tratta di un flusso di dati indirizzato ai portatori di interessi dell'ENISA, con l'intento di sostenere l'attuazione delle politiche e della legislazione dell'UE. In questi flussi di dati si trovano le informazioni raccolte dall'ENISA, provenienti, per la maggior parte del tempo, da fonti pubbliche, e sulla base delle quali l'Agenzia effettua delle analisi condividendone i risultati con i suoi portatori di interessi. L'ENISA svolge alcuni compiti anche su richiesta della Commissione.	Articolo 5, paragrafo 1, lettere a), b), c), e), f) e h) Articolo 5, paragrafo 2; Articolo 5, paragrafo 3; Articolo 5, paragrafo 5 Articolo 6 Articolo 7 Articolo 8 Articolo 9 Articolo 10 Articolo 11, paragrafo 2 Articolo 11, paragrafo 4 Articolo 14
Flussi di dati tra la Commissione, l'ENISA, gli Stati membri e altri soggetti pertinenti all'interno dell'ecosistema di cibersecurity dell'UE, nell'ottica di una cooperazione operativa.	Questo tipo di flussi di dati è destinato a favorire una cooperazione operativa e a garantire una conoscenza situazionale. Lo scambio di informazioni avviene in entrambe le direzioni, in entrata e in uscita. Lo scambio riguarda dati operativi.	Articolo 10, paragrafo 4, lettere da a) a g) Articolo 11, paragrafo 1, lettere da b) a g) Articolo 11, paragrafo 2, lettere a) e b) Articolo 11, paragrafo 3 Articolo 15 Articolo 16, paragrafo 2, lettera e)
Flussi di dati a sostegno dell'ECSF nonché dell'attuazione dei sistemi europei di attestazione delle competenze individuali in materia di cibersecurity	Questi flussi di dati permettono lo scambio di informazioni, sia in entrata che in uscita, per: - il mantenimento e la diffusione dell'ECSF, con flussi tra l'ENISA e i membri dei suoi gruppi di lavoro ad hoc e tra l'ENISA e la Commissione; - lo sviluppo e il mantenimento dei sistemi europei di attestazione delle competenze	Articoli da 19 a 23 Articoli da 36 a 43

	individuali in materia di cibersicurezza, con flussi tra l'ENISA e i membri dei suoi gruppi di lavoro ad hoc nonché tra l'ENISA, la Commissione e gli Stati membri; - l'attuazione dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza, con flussi di dati tra i richiedenti e l'ENISA; - lo scambio di dati tra la commissione di ricorso, l'ENISA, la Commissione e i richiedenti.	
Dati pertinenti agli obiettivi, alle finalità e al contenuto dei sistemi europei di certificazione della cibersicurezza	Questo tipo di flussi di dati è pertinente per la pianificazione, la richiesta, lo sviluppo, l'adozione e il mantenimento (compreso l'eventuale riesame) di sistemi europei di certificazione della cibersicurezza, e deriva in particolare dal coinvolgimento e dalle consulenze specialistiche dei portatori di interessi, dell'ENISA e delle autorità degli Stati membri attraverso l'ECCG in varie fasi della procedura. Altri flussi di dati permettono di fornire informazioni pertinenti al pubblico attraverso siti web dedicati della Commissione e dell'ENISA. Infine il quadro di riferimento prevede la messa a disposizione del pubblico di informazioni supplementari sulla cibersicurezza da parte dei fabbricanti o dei fornitori di prodotti TIC, servizi TIC o processi TIC per i quali questi ultimi abbiano rilasciato, con mezzi propri, una dichiarazione UE di conformità o un certificato europeo di cibersicurezza.	Articolo 18 Articolo 19 Articoli 72, 73, 74, 75, 76, 77, 79, 81, 83, 84

Dati relativi alla governance del quadro europeo di certificazione della cibersecurity	Questi flussi di dati permettono lo scambio di informazioni, sia in entrata che in uscita, per: - il coordinamento e la gestione dei sistemi europei di certificazione della cibersecurity; - l'accreditamento e l'autorizzazione degli organismi di valutazione della conformità nonché la loro successiva notifica attraverso una piattaforma pertinente e le relative procedure; - procedure di ricorso quali il diritto di presentare un reclamo o un ricorso giurisdizionale oppure di appellarsi per richiedere la modifica di procedure	Articoli 85, 86, 88, 89, 90, 92, 93, 94, 95 e 96
Flussi di dati relativi alle attività amministrative dell'Agenzia	Flussi tra l'ENISA, il consiglio di amministrazione, gli Stati membri e la Commissione. Le informazioni riguardano le attività amministrative dell'Agenzia e sono scambiate in entrambe le direzioni. In alcuni casi le informazioni sono trasmesse anche al Parlamento europeo (flusso di dati descritto in appresso).	Articolo 25 Articolo 28, paragrafo 1 Articolo 30 Articolo 31, paragrafo 8 Articolo 32, paragrafi 3 e 5 Articolo 35, paragrafi 5 e 6 Articoli da 36 a 43 Articolo 44 Articolo 45
Dati trasmessi al Parlamento europeo	Flussi di dati trasmessi al Parlamento europeo riguardanti le attività dell'ENISA e lo svolgimento dei suoi compiti, la gestione finanziaria e del bilancio, la cooperazione con i paesi terzi e le organizzazioni internazionali, l'audizione del candidato alla carica di direttore esecutivo e le questioni relative alla certificazione europea della cibersecurity	Articolo 28, paragrafo 1, lettera f), articolo 31, paragrafo 8, articolo 32, paragrafo 3, articolo 44, paragrafo 3, articolo 49, paragrafo 6, articolo 49, paragrafo 9, articolo 70, paragrafo 5, articolo 72, paragrafi 4 e 5, articolo 119, paragrafo 3, Esercizio della delega, articolo 120 Valutazione e riesame

Dati trasmessi al Consiglio dell'UE	Flussi di dati trasmessi al Parlamento europeo riguardanti le attività dell'ENISA e lo svolgimento dei suoi compiti, la gestione finanziaria e del bilancio, la cooperazione con i paesi terzi e le organizzazioni internazionali, l'audizione del candidato alla carica di direttore esecutivo e le proposte di sistemi in fase di sviluppo a norma del quadro europeo di certificazione della cibersicurezza.	Articolo 28, paragrafo 1, lettera f), articolo 31, paragrafo 8, articolo 32, paragrafi 3 e 7, articolo 49, paragrafi 6 e 9, articolo 70, paragrafo 5, articolo 72, paragrafi 4 e 5, articolo 119, paragrafo 3, Esercizio della delega, articolo 120 Valutazione e riesame
Flussi di dati in relazione alla presentazione di un reclamo	Per trattare i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità a norma dell'articolo 84, paragrafo 4, o in relazione alle dichiarazioni UE di conformità. Le persone fisiche e giuridiche hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di cibersicurezza o, se il reclamo riguarda un certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità, all'autorità nazionale di certificazione della cibersicurezza competente.	Articolo 55, paragrafo 3; Articolo 88, paragrafo 7, lettera f); Articolo 96
Flussi di dati relativi ad attacchi ransomware	Segnalazione di determinate informazioni in caso di attacchi ransomware	Articolo 1, punto 8), della direttiva

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
--------------	-------------------------------	---------------------	-------------------	------------------------------	-------------------------

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
Flussi di dati tra la Commissione e gli Stati membri nel contesto dello svolgimento di valutazioni coordinate a livello dell'Unione dei rischi per la sicurezza.	Articolo 99 Valutazioni dei rischi per la sicurezza	Commissione e Stati membri	Stati membri (gruppo di cooperazione NIS)	Articolo 99 Valutazioni dei rischi per la sicurezza	N/D
Flussi di dati tra la Commissione e il Consiglio in relazione alla designazione di paesi terzi che destano preoccupazioni per la cibersecurity	Articolo 100 Designazione dei paesi terzi che destano preoccupazioni per la cibersecurity	Commissione	Consiglio	Articolo 100 Verifica da parte della Commissione della minaccia rappresentata da un paese terzo	
Flussi di dati tra la Commissione e gli Stati membri in relazione all'adozione di misure di mitigazione in caso di circostanze eccezionali	Articolo 103, paragrafo 6 Misure di attenuazione nelle catene di approvvigionamento delle TIC	Commissione	Stati membri	Circostanze eccezionali	N/D
Flussi di dati tra la Commissione e i fornitori e tra la Commissione e le autorità competenti per quanto riguarda la valutazione del luogo di stabilimento nonché dell'assetto	Articolo 104, paragrafi 4, 5 e 6 Individuazione dei fornitori ad alto rischio	Fornitori Commissione Autorità competenti	Autorità competenti Fornitori Commissione	Atti di esecuzione adottati a norma dell'articolo 103, paragrafo 1, e in relazione al divieto di cui	N/D

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
proprietario e di controllo dei fornitori				all'articolo 111, paragrafo 1	
Flusso di dati tra la Commissione e gli Stati membri in relazione ai poteri di vigilanza esercitati nel contesto dell'attuazione di un quadro affidabile in materia di sicurezza delle catene di approvvigionamento delle TIC	Articolo 112, paragrafi 1 e 4 Autorità competenti Articolo 114 Misure di vigilanza e di esecuzione	Stati membri	Commissione	Articolo 112, paragrafi 1 e 4 Autorità competenti Articolo 114 Misure di vigilanza e di esecuzione (la Commissione, in cooperazione con gli Stati membri, pubblica un elenco dei soggetti collegati a fornitori ad alto rischio).	N/D
Flusso di dati tra la Commissione e terzi in caso di esenzioni	Articolo 105 Esenzione dei soggetti stabiliti in un paese terzo che destano preoccupazioni per la cibersecurity o controllati da tale paese terzo	Terzi (soggetti stabiliti in un paese terzo che destano preoccupazioni per la cibersecurity o controllati da soggetti di tale paese terzo) (ai	Commissione (al momento del ricevimento della domanda di esenzione) Terzi (soggetti stabiliti in un paese terzo che destano	Decisione a norma dell'articolo 100 Designazione dei paesi terzi che destano preoccupazioni per la cibersecurity	N/D

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
		sensi dell'articolo 100) (al momento della presentazione di una richiesta di esenzione) Commissione europea (al momento dell'adozione di decisioni)	preoccupazioni per la cibersicurezza o controllati da soggetti di tale paese terzo) (ai sensi dell'articolo 100) (al momento del ricevimento della decisione della Commissione)		
Flusso di dati tra Stati membri e terzi in relazione ai divieti riguardanti le reti di comunicazione elettronica	Articolo 111 Divieti per le reti di comunicazione elettronica mobili, fisse e satellitari	Stati membri (autorità competenti)	Terzi (Fornitori di reti di comunicazione elettronica mobili, fisse e satellitari)	L'autorità competente designata a norma del presente regolamento informa senza ritardo l'autorità competente a norma del regolamento (UE) XX/XXXX [proposta di regolamento sulle reti digitali] in	N/D

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
				merito alle misure imposte ai fornitori di reti di comunicazione elettronica mobili, fisse e satellitari	
Flusso di dati tra la Commissione e gli Stati membri nel contesto della rete dei servizi di cooperazione e di sostegno	Articolo 113 Rete dei servizi di cooperazione e di sostegno della Commissione	Commissione Stati membri (autorità competenti)	Commissione Stati membri (autorità competenti)	Designazione dei paesi terzi che destano preoccupazioni per la cibersecurity	
Flusso di dati tra Stati membri e terzi in relazione alle misure di vigilanza e di esecuzione	Articolo 114 Misure di vigilanza e di esecuzione	Terzi (soggetti del tipo di cui agli allegati I e II della direttiva (UE) 2022/2555)	Stati membri (autorità competenti)	Attuazione delle misure previste al titolo IV	
Flusso di dati tra Stati membri ai fini dell'assistenza reciproca	Articolo 116 Assistenza reciproca	Stati membri	Stati membri	Se un soggetto di cui all'allegato I o II della direttiva (UE) 2022/2555 fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e le sue risorse TIC	N/D

Tipo di dati	Riferimenti alle prescrizioni	Chi fornisce i dati	Chi riceve i dati	Motivo dello scambio di dati	Frequenza (se del caso)
				chiave sono ubicate in uno o più Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità.	

4.3. Soluzioni digitali

Descrizione ad alto livello delle soluzioni digitali

Per ciascuna soluzione digitale, spiegare il modo in cui la soluzione digitale è conforme alle politiche digitali e agli atti legislativi applicabili

Soluzione digitale	Riferimenti alle prescrizioni	Principali funzionalità prescritte	Organismo responsabile	Come si provvede all'accessibilità?	Come viene presa in considerazione l'esigenza della riutilizzabilità?	Uso di tecnologie di IA (se del caso)
L'ENISA svolge la funzione di segretariato della rete di CSIRT e di EU-CyCLONe e utilizza per entrambe le reti strumenti di comunicazione sicura forniti da soggetti giuridici che non sono stabiliti in paesi terzi o che non sono controllati da tali paesi terzi	Articolo 10, paragrafi 2, 3 e 5	Informazioni non pubbliche	ENISA	Informazioni non pubbliche	Informazioni non pubbliche	Informazioni non pubbliche

o da cittadini di paesi terzi.						
Sviluppare, in cooperazione con EU-CyCLONe, la rete di CSIRT, la Commissione, Europol, il CERT-UE e altri soggetti pertinenti dell'Unione, archivi di intelligence verificata e affidabile sulle minacce informatiche , comprese le tendenze in materia di incidenti, tattiche, tecniche e procedure.	Articolo 11, paragrafo 1, lettera a)	intelligence verificata e affidabile sulle minacce informatiche, comprese le tendenze in materia di incidenti, tattiche, tecniche e procedure	ENISA EU-CyCLONe, la rete di CSIRT, la Commissione, Europol, il CERT-UE e altri soggetti pertinenti dell'Unione	N/D	N/D	N/D
L'ENISA mantiene un archivio degli insegnamenti tratti.	Articolo 14, paragrafo 2	L'ENISA mantiene un archivio degli insegnamenti tratti dalle esercitazioni svolte e formula raccomandazioni rivolte agli Stati membri e, se del caso, ai soggetti dell'Unione in merito a come mettere in pratica in modo efficace ed efficiente tali insegnamenti.	ENISA	N/D	N/D	N/D

L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, come le piattaforme relative alla cibersecurity a livello dell'Unione, in particolare la piattaforma unica di segnalazione istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 [e il punto di accesso unico per la segnalazione degli incidenti istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555], oppure strumenti di prova a sostegno dell'attuazione delle procedure di valutazione della conformità a norma della pertinente normativa dell'Unione.	Articolo 15	Piattaforma unica di segnalazione Articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 [punto di accesso unico articolo 23 bis della direttiva (UE) 2022/2555]	ENISA	N/D	N/D	N/D
Mantenere la banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555 e fornire servizi di gestione delle vulnerabilità	Articolo 16, paragrafo 2	Articolo 12, paragrafo 2, della direttiva (UE) 2022/2555 Mantenere la banca dati e fornire servizi di gestione delle vulnerabilità	ENISA	N/D	N/D	N/D
L'ENISA gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni pubbliche	Articoli da 19 a 23	Mantenere e aggiornare regolarmente un apposito sito web che fornisca informazioni pubbliche riguardanti l'ECSF, comprendenti il quadro e il relativo calendario di	ENISA	N/D	N/D	N/D

		aggiornamento; i sistemi europei di attestazione delle competenze individuali in materia di cibersecurity, i progressi compiuti e le tempistiche per il loro sviluppo; i diritti associati a ciascun sistema europeo di attestazione delle competenze individuali in materia di cibersecurity; il costo indicativo di un attestato europeo delle competenze individuali in materia di cibersecurity; l'elenco dei fornitori autorizzati di attestati.				
La Commissione gestisce e aggiorna regolarmente un apposito sito web pubblico	Articolo 72	Informazioni trasmesse: a) sistemi europei di certificazione della cibersecurity di cui è stato richiesto lo sviluppo; b) priorità strategiche per l'armonizzazione dei prodotti TIC, dei servizi	Commissione europea	Rispetto degli orientamenti	Rispetto degli orientamenti	N/D

		TIC, dei processi TIC, dei servizi di sicurezza gestiti o dei requisiti di sicurezza della normativa dell'Unione, compresi i potenziali settori per i quali potrebbe essere richiesto un sistema europeo di certificazione della cibersecurity.				
L'ENISA gestisce un apposito sito web sulla certificazione	Articolo 79	Fornisce informazioni: a) sui sistemi europei di certificazione della cibersecurity; b) sui diritti associati al mantenimento di ciascun sistema europeo di certificazione della cibersecurity; c) sulle pertinenti specifiche tecniche dell'ENISA; d) sui certificati europei di cibersecurity e sulle dichiarazioni UE di conformità, comprese informazioni sui certificati e sulle dichiarazioni che non	ENISA	Rispetto degli orientamenti	Rispetto degli orientamenti	N/D

		sono più validi o che sono sospesi, revocati o scaduti; e) sulle informazioni supplementari sulla cibersecurity pertinenti in conformità dell'articolo 84, paragrafo 2; f) sulle sintesi delle revisioni tra pari a norma dell'articolo 89, paragrafo 7; g) sulle specifiche tecniche richiamate in un sistema europeo di certificazione della cibersecurity a norma dell'articolo 74, paragrafo 10.				
Registro (delle esenzioni per i soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersecurity o controllati da soggetti di tale paese terzo)	Articolo 107 Registro	La Commissione tiene un registro accessibile al pubblico delle decisioni adottate a norma dell'articolo 105, paragrafo 4. Il registro riporta i nomi dei soggetti destinatari delle decisioni. La	Commissione	"La Commissione tiene un registro accessibile al pubblico"	N/D	N/D

		Commissione lo aggiorna regolarmente.				
Piattaforma (per la cooperazione e lo scambio di informazioni tra la Commissione e le autorità competenti)	Articolo 113	La Commissione istituisce una rete di cooperazione tra le autorità competenti degli Stati membri e la Commissione, che funga da piattaforma per la cooperazione e lo scambio di informazioni. La Commissione fornisce alla rete sostegno amministrativo.	Commissione	Informazioni non accessibili pubblico, ma solo alle autorità competenti	N/D	N/D
L'ENISA crea e mantiene un registro dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio	Articolo 1, punto 11), della direttiva	Registro dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio	ENISA	N/D	Sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 2 (articolo 27	N/D

					della direttiva NIS 2)	
--	--	--	--	--	------------------------	--

Soluzioni digitali incluse nella tabella precedente

Politica digitale e/o settoriale (se applicabili)	Spiegazione sull'allineamento della soluzione alla politica in questione
<i>Regolamento sull'IA</i>	N/D
<i>Quadro dell'UE in materia di cibersecurity</i>	N/D
<i>eIDAS</i>	N/D
<i>Sportello digitale unico e IMI</i>	N/D
<i>Altri</i>	N/D

Descrizione ad alto livello dei servizi pubblici digitali interessati dalle prescrizioni

Servizio pubblico digitale o categoria di servizi pubblici digitali	Descrizione	Riferimenti alle prescrizioni	Soluzioni per un'Europa interoperabile (NON APPLICABILE)	Altre soluzioni di interoperabilità
L'ENISA svolge la funzione di segretariato delle reti e si occupa di diffondere strumenti di comunicazione sicura	L'ENISA svolge la funzione di segretariato della rete di CSIRT a norma dell'articolo 15, paragrafo 2, della direttiva (UE) 2022/2555. L'ENISA svolge la funzione di segretariato di EU-CyCLONe a norma dell'articolo 16, paragrafo 2, della direttiva (UE) 2022/2555 [e fornisce un punto di	Articolo 11	//	N/D

	accesso unico per la segnalazione degli incidenti istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555] nonché strumenti di prova a sostegno dell'attuazione delle procedure di valutazione della conformità a norma della pertinente legislazione dell'Unione. Nell'ambito della rete di CSIRT e di EU-CyCLONe, l'ENISA utilizza strumenti di comunicazione sicura forniti da soggetti giuridici che non sono stabiliti in paesi terzi o che non sono controllati da tali paesi terzi o da cittadini di paesi terzi.			
Allerte precoci	Emissione di allerte precoci	Articolo 11 Articolo 12		
Sostegno in relazione a uno specifico incidente informatico o una specifica minaccia informatica, potenziale o in corso	Su richiesta di uno o più Stati membri, fornire consulenza e valutazioni in relazione a uno specifico incidente informatico o una specifica minaccia informatica, potenziale o in corso, anche tramite la messa a disposizione di competenze e l'agevolazione della gestione tecnica di tali incidenti, e il sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri.	Articolo 10		
Sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala	Contribuire a sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala, in particolare assistendo EU-CyCLONe nella redazione di relazioni a livello politico e agevolando la condivisione tempestiva delle informazioni tra la rete di CSIRT	Articolo 10		

	e EU-CyCLONe			
Archivi di intelligence verificata e affidabile sulle minacce informatiche	Sviluppare, in cooperazione con EU-CyCLONe, la rete di CSIRT, la Commissione, Europol, il CERT-UE e altri soggetti pertinenti dell'Unione, archivi di intelligence verificata e affidabile sulle minacce informatiche, comprese le tendenze in materia di incidenti, tattiche, tecniche e procedure.	Articolo 11		
Archivio degli insegnamenti tratti	L'ENISA mantiene un archivio degli insegnamenti tratti dalle esercitazioni svolte e formula raccomandazioni rivolte agli Stati membri e, se del caso, ai soggetti dell'Unione in merito a come mettere in pratica in modo efficace ed efficiente tali insegnamenti.	Articolo 14		
L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, quali le piattaforme	L'ENISA istituisce, fornisce, gestisce, mantiene e aggiorna, se necessario, strumenti tecnici operativi, come le piattaforme relative alla cibersecurity a livello dell'Unione, in particolare la piattaforma unica di segnalazione istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 [e il punto di accesso unico per la segnalazione degli incidenti istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555], nonché strumenti di prova a sostegno dell'attuazione delle procedure di valutazione della conformità a norma della pertinente normativa dell'Unione.	Articolo 15		
Mantenere la banca dati europea delle vulnerabilità istituita a	Mantenere la banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della	Articolo 16		

norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555	direttiva (UE) 2022/2555. Fornire servizi di gestione delle vulnerabilità ai portatori di interessi, basandosi sulla banca dati europea delle vulnerabilità e utilizzando le informazioni pertinenti di cui dispone l'ENISA. Avviare una cooperazione strutturata con organizzazioni che forniscono programmi, registri o banche dati simili alla banca dati europea delle vulnerabilità. Assistere attivamente i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555 per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro. Sviluppare e mantenere metodologie e meccanismi di governance per l'individuazione e la divulgazione coordinata delle vulnerabilità, in cooperazione con le autorità nazionali competenti, i CSIRT, l'industria e la comunità della ricerca.			
Preparare proposte di sistemi europei di certificazione della cibersecurity ("proposte di sistemi")	Preparare proposte di sistemi europei di certificazione della cibersecurity ("proposte di sistemi") per prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti e le relative specifiche tecniche conformemente all'articolo 74. Mantenere i sistemi europei di	Articolo 17		

	certificazione della cibersicurezza adottati conformemente all'articolo 75, anche in considerazione di un'eventuale revisione di tali sistemi a norma dell'articolo 76.			
L'ENISA sviluppa e mantiene sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza	L'ENISA sviluppa e mantiene sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza. L'ENISA adotta una decisione motivata tramite cui concede al richiedente l'autorizzazione a rilasciare attestati individuali europei per la fornitura e il mantenimento dei sistemi e dell'autorizzazione, nega l'autorizzazione o chiude il processo d'esame della domanda a causa dell'insufficienza delle informazioni fornite dal richiedente o della sua inerzia a seguito di una richiesta di informazioni supplementari.	Articoli 20 e 22		
L'ENISA gestisce e aggiorna regolarmente un apposito sito web	L'ENISA gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni pubbliche riguardanti: a) l'ECSF, comprendenti il quadro e il relativo calendario di aggiornamento; b) i sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza, i progressi compiuti e le tempistiche per il loro sviluppo; c) i diritti associati a ciascun sistema europeo di attestazione delle	Articolo 23		

	competenze individuali in materia di cibersecurity adottato a norma dell'articolo 47 del presente regolamento; d) il costo indicativo di un attestato europeo delle competenze individuali in materia di cibersecurity a norma dell'articolo 20, paragrafo 4; e) l'elenco dei fornitori autorizzati di attestati.			
La Commissione gestisce e aggiorna regolarmente un apposito sito web pubblico	La Commissione gestisce e aggiorna regolarmente un apposito sito web che fornisce informazioni sui seguenti aspetti: a) sistemi europei di certificazione della cibersecurity di cui è stato richiesto lo sviluppo; b) priorità strategiche per l'armonizzazione dei prodotti TIC, dei servizi TIC, dei processi TIC, dei servizi di sicurezza gestiti o dei requisiti di sicurezza della normativa dell'Unione, compresi i potenziali settori per i quali potrebbe essere richiesto un sistema europeo di certificazione della cibersecurity.	Articolo 72		
L'ENISA gestisce un apposito sito web sulla certificazione	L'ENISA gestisce e aggiorna periodicamente un apposito sito web che fornisce informazioni pubbliche: a) sui sistemi europei di certificazione della cibersecurity; b) sui diritti associati al mantenimento di ciascun sistema europeo di certificazione della cibersecurity; c) sulle pertinenti specifiche tecniche dell'ENISA;	Articolo 79		

	d) sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità, comprese informazioni sui certificati e sulle dichiarazioni che non sono più validi o che sono sospesi, revocati o scaduti; e) sulle informazioni supplementari sulla cibersicurezza pertinenti in conformità dell'articolo 84, paragrafo 2; f) sulle sintesi delle revisioni tra pari a norma dell'articolo 89, paragrafo 7; g) sulle specifiche tecniche richiamate in un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 74, paragrafo 10.			
Inchieste	La Commissione indaga sui casi in cui abbia dubbi o venga a conoscenza di dubbi sulla competenza di un organismo di valutazione della conformità ad adempiere le prescrizioni e le responsabilità che ad esso incombono, o sul continuo adempimento, da parte di tale organismo, di tali prescrizioni e responsabilità. La Commissione garantisce la riservatezza di tutte le informazioni sensibili raccolte nel corso delle sue indagini.	Articolo 94		
L'ENISA crea e mantiene un registro dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio	Registro dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Su richiesta, l'ENISA consente alle autorità competenti di accedere alle informazioni conservate in tale registro riguardanti i fornitori di servizi DNS, i	Articolo 1, punto 11), della direttiva		

	registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, assicurando nel contempo la tutela della riservatezza delle informazioni, se del caso.			
--	---	--	--	--

4.4. Valutazione dell'interoperabilità

Impatto delle prescrizioni come da servizio pubblico digitale sull'interoperabilità transfrontaliera

Archivi/piattaforme/allerte precoci/segretariato/cooperazione operativa/banca dati per la divulgazione coordinata delle vulnerabilità

Valutazione	Misure	Potenziati ostacoli residui
Valutare l'allineamento con le politiche digitali e settoriali in vigore Elencare le politiche digitali e settoriali pertinenti individuate	<i>Cybersicurezza</i>	<i>Nessun ostacolo noto</i>
Valutare le misure organizzative per un'agevole prestazione dei servizi pubblici digitali transfrontalieri Elencare le misure di governance previste	<i>Consiglio di amministrazione dell'ENISA</i> <i>Rete di CSIRT</i> <i>EU-CyCLONe</i> <i>Gruppo di cooperazione NIS</i> <i>Si tratta di sedi di discussione di questioni pertinenti.</i>	<i>N/D</i>
Valutare le misure adottate per		

assicurare un'interpretazione condivisa dei dati Elencare tali misure	N/D	N/D
Valutare l'uso di norme e specifiche tecniche aperte concordate Elencare tali misure	N/D	N/D

Sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza

Valutazione	Misure	Potenziali ostacoli residui
Valutare l'allineamento con le politiche digitali e settoriali in vigore Elencare le politiche digitali e settoriali pertinenti individuate	<i>La proposta si basa sul documento COM(2023) 207 final (Accademia per le competenze in materia di cibersicurezza): "l'ENISA metterà a punto un progetto pilota che valuterà l'istituzione di un sistema europeo di attestazione delle competenze in materia di cibersicurezza".</i> <i>Si basa inoltre sul regolamento (UE) 2024/1183 (portafoglio EUDI) stabilendo che l'ENISA e i fornitori autorizzati di attestati garantiscono il rilascio di attestati elettronici degli attestati europei delle competenze individuali in materia di cibersicurezza nei portafogli europei di identità digitale.</i> <i>Cibersicurezza</i> <i>GDPR (conservazione dei registri da parte dei soggetti autorizzati)</i>	Nessun ostacolo noto
Valutare le misure organizzative per un'agevole prestazione dei servizi pubblici digitali transfrontalieri Elencare le misure di governance previste	<i>Consultazione dei portatori di interessi durante la messa a punto di un sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza</i> <i>Ripartizione dei compiti all'interno dell'ENISA</i>	<i>L'uso e il riconoscimento dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza rimangono volontari per i soggetti pubblici e privati.</i>

	<i>per garantire che siano svolti in modo indipendente</i> <i>Commissione di ricorso</i>	
Valutare le misure adottate per assicurare un'interpretazione condivisa dei dati Elencare tali misure	<i>Mettere a punto sistemi che specifichino, tra l'altro, le norme relative al contenuto e al formato degli attestati</i> <i>I soggetti autorizzati garantiscono che, su richiesta dell'interessato, gli attestati europei delle competenze individuali in materia di cibersecurity siano rilasciati sotto forma di attestati elettronici di attributi in un formato che può essere archiviato nei portafogli europei di identità digitale. L'ENISA fornisce orientamenti ai valutatori e impartisce loro una formazione obbligatoria in merito ai requisiti e ai metodi di valutazione previsti nel sistema europeo di attestazione delle competenze individuali in materia di cibersecurity.</i> <i>Fornire informazioni pubbliche su un sito web</i> <i>Adozione di atti di esecuzione riguardanti i diritti riscossi</i>	<i>Anche se i sistemi dovrebbero essere tanto dettagliati da garantire una comprensione comune e facilitare l'attuazione e anche se l'ENISA fornirà orientamenti ai valutatori e impartirà loro una formazione obbligatoria per garantire un'attuazione coerente dei sistemi, potrebbero emergere problematiche impreviste che porterebbero i fornitori autorizzati di attestati a dover interagire con l'ENISA, altri soggetti autorizzati o valutatori.</i>
Valutare l'uso di norme e specifiche tecniche aperte concordate Elencare tali misure	<i>Sviluppo di sistemi europei di attestazione delle competenze individuali in materia di cibersecurity con il sostegno dei pertinenti portatori di interessi</i>	N/D

Preparare proposte di sistemi europei di certificazione della cibersecurity ("proposte di sistemi")/assegnare numeri di identificazione agli organismi di valutazione della conformità

Valutazione	Misure	Potenziali ostacoli residui
Valutare l'allineamento con le politiche digitali e settoriali in vigore Elencare le politiche digitali e settoriali pertinenti individuate	<i>La proposta mira a un allineamento in materia di governance con il nuovo quadro legislativo, in particolare per quanto riguarda il regolamento (CE) n. 765/2008²⁶. La proposta mira a favorire il rispetto della pertinente legislazione settoriale in materia di ciphersicurezza attraverso lo sviluppo di appositi sistemi europei di certificazione della ciphersicurezza.</i>	<i>Nessun ostacolo noto</i>
Valutare le misure organizzative per un'agevole prestazione dei servizi pubblici digitali transfrontalieri Elencare le misure di governance previste	<i>Gruppo europeo per la certificazione della ciphersicurezza; ENISA; gruppi di lavoro ad hoc; assemblea europea sulla certificazione della ciphersicurezza; consultazione dei portatori di interessi al momento della richiesta, dello sviluppo e dell'adozione di sistemi europei di certificazione della ciphersicurezza; procedure di comitato per atti di esecuzione previsti relativi a sistemi europei di certificazione della ciphersicurezza.</i>	<i>Il ricorso alla certificazione europea della ciphersicurezza è volontario, salvo diversamente specificato nella legislazione europea.</i>
Valutare le misure adottate per assicurare un'interpretazione condivisa dei dati Elencare tali misure	<i>Atti di esecuzione elencati nella sezione 4.5.</i>	<i>Il ricorso alla certificazione europea della ciphersicurezza è volontario, salvo diversamente specificato nella legislazione europea.</i>
Valutare l'uso di norme e specifiche tecniche aperte concordate Elencare tali misure	<i>Atti di esecuzione elencati nella sezione 4.5. I requisiti specificati del sistema europeo di certificazione della ciphersicurezza sono coerenti con le prescrizioni della legislazione dell'Unione. I sistemi europei di certificazione della</i>	<i>N/D</i>

	<i>cybersicurezza fanno riferimento alle norme internazionali, europee o nazionali applicate nella valutazione o, qualora tali norme non siano disponibili o adeguate, alle specifiche tecniche elaborate dall'ENISA.</i>	
--	---	--

Siti web accessibili al pubblico

Valutazione	Misure	Potenziali ostacoli residui
Valutare l'allineamento con le politiche digitali e settoriali in vigore Elencare le politiche digitali e settoriali pertinenti individuate	<i>Atto europeo sull'accessibilità e direttiva sull'accessibilità del web</i> <i>Cybersicurezza</i>	<i>Nessun ostacolo noto</i>
Valutare le misure organizzative per un'agevole prestazione dei servizi pubblici digitali transfrontalieri Elencare le misure di governance previste	<i>N/D</i>	<i>N/D</i>
Valutare le misure adottate per assicurare un'interpretazione condivisa dei dati Elencare tali misure		<i>N/D</i>
Valutare l'uso di norme e specifiche tecniche aperte concordate Elencare tali misure		<i>N/D</i>

4.5. Misure a sostegno dell'attuazione digitale

Descrizione ad alto livello delle misure a sostegno dell'attuazione digitale

Descrizione della misura	Riferimenti alle prescrizioni	Ruolo della Commissione	Chi deve essere coinvolto	Calendario previsto (se del caso)
---------------------------------	--------------------------------------	--------------------------------	----------------------------------	--

		(se del caso)	(se del caso)	
Sulla base della proposta di sistema preparata dall'ENISA e accolta, la Commissione ha il potere di adottare atti di esecuzione, prevedendo un sistema europeo di certificazione della cibersecurity per i prodotti TIC, i servizi TIC, i processi TIC, i servizi di sicurezza gestiti o la postura di cibersecurity dei soggetti che soddisfa i requisiti di cui agli articoli 80 e 81. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.	Articolo 75, paragrafo 9	Alla Commissione è conferito il potere di adottare atti di esecuzione		N/D
Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 119 per modificare il paragrafo 1 del presente articolo aggiungendo o modificando obiettivi di sicurezza al fine di garantire che riflettano i più recenti sviluppi tecnologici e le nuove minacce correlate, nonché l'adozione di una nuova normativa dell'Unione che stabilisce che la certificazione europea della cibersecurity possa essere utilizzata per dimostrare la presunzione di conformità ai pertinenti requisiti di cibersecurity di tale normativa.	Articolo 80, paragrafo 2	Alla Commissione è conferito il potere di adottare atti delegati		N/D
Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscano principi comuni e disposizioni tipo per gli elementi di cui ai paragrafi 1, 2 e 3 in tutti i	Articolo 81, paragrafo 5	Alla Commissione è conferito il potere di adottare atti di esecuzione	ENISA ECCG	N/D

sistemi europei di certificazione della cibersecurity. Un sistema europeo di certificazione della cibersecurity può includere riferimenti a tali principi e disposizioni tipo, se del caso e ove disponibili. Gli atti di esecuzione di cui al primo comma sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2. Nell'elaborare o rivedere i principi comuni e le disposizioni tipo per gli elementi dei sistemi europei di certificazione della cibersecurity, la Commissione consulta l'ENISA e tiene conto, se del caso, delle opinioni dell'ECCG, dei pertinenti portatori di interessi e di altri organismi pertinenti.				
Alla Commissione è conferito il potere di adottare atti di esecuzione che specifichino le procedure per il modello di previa approvazione o di delega generale di cui al paragrafo 4 del presente articolo. Nell'elaborare tali atti di esecuzione la Commissione consulta l'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.	Articolo 85, paragrafo 5	Alla Commissione è conferito il potere di adottare atti di esecuzione	ECCG	N/D
I certificati di paesi terzi relativi a prodotti TIC, servizi TIC, processi TIC, servizi di sicurezza gestiti e alla postura di	Articolo 87, paragrafo 1	Alla Commissione è conferito il potere di adottare atti di		N/D

cibersicurezza dei soggetti possono essere riconosciuti, mediante un atto di esecuzione o attraverso la conclusione di un accordo tra l'Unione e il paese terzo in questione o un'organizzazione internazionale, come equivalenti ai certificati europei di cibersicurezza se i requisiti del pertinente sistema del paese terzo o dell'organizzazione internazionale sono considerati equivalenti a quelli dei sistemi europei di certificazione della cibersicurezza. Alla Commissione è conferito il potere di adottare tali atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.		esecuzione		
Alla Commissione è conferito il potere di adottare atti di esecuzione che definiscano un piano almeno quinquennale per la revisione tra pari e fissino i criteri riguardanti la composizione del gruppo incaricato della revisione tra pari, la metodologia da utilizzare in tale revisione nonché il calendario, la frequenza e altri compiti ad essa connessi. Nell'elaborare tali atti di esecuzione la Commissione consulta l'ECCG e l'ENISA. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.	Articolo 89, paragrafo 6	Alla Commissione è conferito il potere di adottare atti di esecuzione		N/D
Alla Commissione è conferito il potere di	Articolo 92, paragrafo 8	Alla Commissione è	ENISA	N/D

adottare atti di esecuzione per stabilire le procedure, anche in materia di cooperazione transfrontaliera, per l'autorizzazione degli organismi di valutazione della conformità. Nell'elaborare gli atti di esecuzione la Commissione consulta l'ENISA e l'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.		conferito il potere di adottare atti di esecuzione	ECCG	
Alla Commissione è conferito il potere di adottare atti di esecuzione per stabilire le circostanze, i formati e le procedure per le notifiche di cui al paragrafo 1 del presente articolo, compresa la procedura di opposizione da parte di altri Stati membri durante il processo di notifica, l'identificazione univoca degli organismi di valutazione della conformità, nonché le circostanze per la limitazione, la sospensione o il ritiro della notifica. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 118, paragrafo 2.	Articolo 93, paragrafo 3	Alla Commissione è conferito il potere di adottare atti di esecuzione		N/D
La Commissione può adottare atti di esecuzione conformemente all'articolo 100 al fine di designare un paese terzo come paese che desta preoccupazioni per la cibersecurity per le catene di approvvigionamento delle TIC.	Articolo 100, paragrafo 2 Designazione dei paesi terzi che destano preoccupazioni per la cibersecurity	Adozione di atti di esecuzione		N/D Nessun calendario, ma gli atti di esecuzione dovrebbero essere riesaminati

				periodicamente
La Commissione può adottare atti di esecuzione per prevedere una o più misure di mitigazione di cui all'articolo 103, paragrafo 2.	Articolo 103, paragrafo 2 Misure di attenuazione nella catena di approvvigionamento delle TIC	Adozione di atti di esecuzione	N/D	N/D Nessun calendario, ma gli atti di esecuzione devono essere riesaminati ogni 36 mesi (secondo la procedura d'esame di cui all'articolo 118, paragrafo 2).
La Commissione può adottare atti di esecuzione conformemente all'articolo 102 al fine di individuare le risorse TIC chiave utilizzate per la fabbricazione di prodotti o la fornitura di servizi da parte delle tipologie di soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555.	Articolo 102, paragrafo 1 Individuazione delle risorse TIC chiave	Adozione di atti di esecuzione	N/D	N/D
La Commissione può adottare atti di esecuzione che vietino di utilizzare, installare o integrare in qualsiasi forma nelle risorse TIC chiave individuate in conformità dell'articolo 102 componenti TIC o componenti che comprendono componenti TIC di fornitori ad alto rischio designati a norma dell'articolo 100, paragrafo 2.	Articolo 103, paragrafo 1 Misure di attenuazione nella catena di approvvigionamento delle TIC	Adozione di atti di esecuzione	N/D	N/D
La Commissione può adottare atti di esecuzione per stabilire che alle tipologie di	Articolo 103, paragrafo 7	Adozione di atti di esecuzione	Consultazione degli Stati membri	N/D

soggetti di cui agli allegati I e II della direttiva (UE) 2022/2555 è vietato utilizzare, installare o integrare componenti TIC o componenti che comprendono componenti TIC di un soggetto specifico.			e dei soggetti interessati	
Mediante atti di esecuzione, la Commissione stila elenchi di fornitori ad alto rischio pertinenti ai fini dei divieti stabiliti negli atti di esecuzione adottati a norma dell'articolo 103, paragrafo 1, o del divieto di cui all'articolo 1110, paragrafo 1.	Articolo 104, paragrafo 1	Adozione di atti di esecuzione	N/D	N/D
La Commissione può adottare atti di esecuzione per specificare ulteriormente le condizioni di cui all'articolo 105, paragrafo 2, lettera b), e per stabilire norme dettagliate riguardo alle procedure di cui all'articolo 105.	Articolo 105 Esenzione per i soggetti stabiliti in un paese terzo che desta preoccupazioni per la cibersicurezza o controllati da soggetti di tale paese terzo	Adozione di atti di esecuzione	N/D	N/D
La Commissione può adottare atti di esecuzione che stabiliscano norme dettagliate relative ai diritti, specificandone l'importo e le modalità di pagamento.	Articolo 109 Diritti	Adozione di atti di esecuzione	N/D	N/D
La Commissione adotta atti di esecuzione per specificare i termini per l'eliminazione graduale dei componenti TIC o dei componenti che comprendono componenti TIC forniti da fornitori ad alto rischio per quanto riguarda le reti di comunicazione elettronica fisse e satellitari.	Articolo 110, paragrafo 4 Risorse TIC chiave per le reti di comunicazione elettronica mobili, fisse e satellitari	Adozione di atti di esecuzione	N/D	N/D
La Commissione può adottare atti delegati	Articolo 110, paragrafo 5	Adozione di atti	N/D	N/D

conformemente all'articolo 119 per modificare l'allegato II in modo da adeguarlo agli sviluppi tecnologici tenendo conto degli elementi di cui all'articolo 103, paragrafo 3.		delegati		
7. L'articolo 21, paragrafo 5, è così modificato: a) il secondo comma è sostituito dal seguente: "La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di cui al paragrafo 2 per quanto riguarda i soggetti essenziali e importanti diversi da quelli di cui al primo comma del presente paragrafo. La Commissione valuta regolarmente se gli atti di esecuzione di cui al presente comma debbano essere adottati per settori specifici o per tipologie specifiche di soggetti al fine di migliorare il funzionamento del mercato interno. Sulla base dell'esito di tali valutazioni, la Commissione può proporre tali atti di esecuzione per le tipologie di soggetti o i settori individuati. Nell'elaborare tali valutazioni, la Commissione si concentra in particolare sulla natura transfrontaliera dei settori o delle tipologie di soggetti e procede a un processo di consultazione aperto, trasparente e inclusivo con i	Articolo 1, punto 7), della direttiva Armonizzazione massima	La Commissione può adottare atti di esecuzione		N/D

pertinenti portatori di interessi e gli Stati membri."; b) dopo il quarto comma, è aggiunto il comma seguente: "Quando la Commissione adotta gli atti di esecuzione di cui al primo e al secondo comma del presente paragrafo, gli Stati membri non impongono ulteriori requisiti tecnici o metodologici relativi alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 ai soggetti che rientrano nell'ambito di applicazione di tali atti di esecuzione."				
---	--	--	--	--