COMMISSIONE
EUROPEA

Bruxelles, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

{SWD(2022) 67 final} - {SWD(2022) 68 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

La presente proposta istituisce un quadro per garantire norme e misure comuni in materia di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione, con lo scopo di migliorare le capacità di resilienza e di risposta agli incidenti di tutti i soggetti in questione. Essa è in linea con le priorità della Commissione di preparare l'Europa per l'era digitale e costruire un'economia pronta per le sfide del futuro e al servizio dei cittadini, garantendo al tempo stesso che una pubblica amministrazione sicura e resiliente sia il fondamento della trasformazione digitale dell'insieme della società.

La proposta si basa sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final) e sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale (JOIN(2020) 18 final).

La proposta modernizza il quadro giuridico esistente relativo al CERT-UE e tiene conto degli sviluppi e dell'aumento della digitalizzazione nelle istituzioni, negli organi e nelle agenzie negli ultimi anni e dell'evolversi del panorama delle minacce alla cibersicurezza. Entrambi i fenomeni si sono ulteriormente amplificati dall'inizio della crisi COVID-19, mentre è in continuo aumento il numero di incidenti, molti dei quali, sempre più sofisticati, provengono da un'ampia gamma di fonti.

La proposta rinomina il CERT-UE da "squadra di pronto intervento informatico" in "centro per la cibersicurezza" delle istituzioni, degli organi e delle agenzie dell'Unione, in linea con gli sviluppi negli Stati membri e a livello globale che vedono molti CERT-UE ribattezzati come "centri per la cibersicurezza", pur mantenendo l'abbreviazione CERT-UE ai fini del riconoscimento del nome.

• Coerenza con le disposizioni vigenti nel settore normativo interessato

La presente proposta è volta ad aumentare la resilienza, in termini di cibersicurezza, delle istituzioni, degli organi e delle agenzie dell'Unione contro le minacce informatiche, allineandosi alla legislazione esistente:

- direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La proposta si allinea anche alla proposta di direttiva (UE) XXXX/XXXX relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 [proposta NIS 2];
- regolamento 2019/881 relativo all'Agenzia dell'Unione europea per la cibersicurezza e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza);
- proposta di regolamento (UE) XXXX/XXXX sulla sicurezza delle informazioni nelle istituzioni, organi e organismi dell'Unione;
- raccomandazione della Commissione, del 23 giugno 2021, sull'istituzione di un'unità congiunta per il ciberspazio;
- raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

L'allegato della raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala definisce il programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala.

Nella sua risoluzione del 9 marzo 2021, il Consiglio dell'Unione europea ha sottolineato che la cibersicurezza è essenziale per il funzionamento della pubblica amministrazione a livello sia nazionale che dell'UE come pure per la società e per l'economia nel loro complesso, mettendo in evidenza l'importanza di un quadro di sicurezza solido e coerente per proteggere il personale, i dati, le reti di comunicazione, i sistemi di informazione e i processi decisionali dell'Unione. A tal fine è necessario in particolare rafforzare la resilienza e migliorare la cultura della sicurezza delle istituzioni, negli organi e nelle agenzie dell'Unione. Devono essere rese disponibili risorse e capacità sufficienti, anche nel contesto del rafforzamento del mandato del CERT-UE.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La base giuridica del presente regolamento è l'articolo 298 del trattato sul funzionamento dell'Unione europea ("TFUE"), secondo il quale nell'assolvere i loro compiti le istituzioni, organi e organismi dell'Unione si basano su un'amministrazione europea aperta, efficace ed indipendente. Il Parlamento europeo e il Consiglio, deliberando mediante regolamenti secondo la procedura legislativa ordinaria, fissano disposizioni a tal fine, nel rispetto dello statuto e del regime adottati sulla base dell'articolo 336.

Le tecnologie dell'informazione hanno introdotto nelle istituzioni, negli organi e nelle agenzie dell'Unione nuovi modi di lavorare, interagire con i cittadini e migliorare il funzionamento generale. La tecnologia continua ad evolvere e il panorama delle minacce informatiche va di pari passo. Le istituzioni, gli organi e le agenzie dell'Unione sono diventati obiettivi molto interessanti di attacchi informatici sofisticati. L'introduzione di sistemi e requisiti per garantire la cibersicurezza sembra contribuire all'efficienza e all'indipendenza dell'amministrazione europea, in modo che le istituzioni, gli organi e gli organismi dell'Unione possano operare e svolgere in modo più efficiente i loro compiti in un mondo digitale.

Le attuali differenze spiegate sotto, nella sezione 3, nella posizione di cibersicurezza e nell'approccio in materia delle istituzioni, degli organi e delle agenzie dell'Unione, costituiscono inoltre ulteriori ostacoli ad un'amministrazione europea aperta, efficace ed indipendente. Senza un approccio comune la posizione di cibersicurezza fra le istituzioni, gli organi e le agenzie dell'Unione continuerebbe ad evolvere in direzioni divergenti. La presente base giuridica è pertanto appropriata, poiché il regolamento è volto a creare un quadro giuridico comune per la cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.

- **Sussidiarietà**

Il regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, organi e organismi dell'Unione rientra nella competenza esclusiva dell'Unione.

- **Proporzionalità**

Le norme proposte nel presente regolamento non vanno oltre ciò che è necessario per raggiungere in modo soddisfacente gli obiettivi specifici. Le misure previste contribuiranno al raggiungimento di un livello comune elevato di cibersicurezza limitandosi a quanto necessario per conseguire l'obiettivo perseguito, alla luce dei rischi sempre più elevati che si presentano.

- **Scelta dell'atto giuridico**

La scelta di un regolamento, che è direttamente applicabile, è considerata lo strumento giuridico adeguato per definire e razionalizzare gli obblighi imposti alle istituzioni, agli organi e alle agenzie dell'Unione. Un regolamento è lo strumento giuridico più appropriato per consentire miglioramenti mirati.

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

- **Valutazioni ex ante**

Il CERT-UE ha effettuato una valutazione delle principali minacce informatiche alle quali le istituzioni, gli organi e le agenzie dell'Unione sono attualmente esposti o saranno verosimilmente esposti nel prossimo futuro.

Nell'analisi sono state utilizzate tre categorie di osservazioni:

- i tentativi di violare le infrastrutture informatiche delle istituzioni, degli organi e delle agenzie dell'Unione (se riusciti sono trattati come incidenti, negli altri casi sono comunque registrati come tentativi individuati);
- le minacce rilevate intorno alle istituzioni, agli organi e alle agenzie dell'Unione (ad esempio in settori collegati, presso i gruppi di portatori di interessi o in Europa);
- le tendenze delle minacce più importanti constatate a livello globale.

L'analisi ha inoltre esaminato in che modo grandi cambiamenti stanno influendo sul modo in cui le istituzioni dell'Unione gestiscono e utilizzano le loro infrastrutture e i loro servizi informatici. Tali cambiamenti includono:

- maggiore telelavoro;
- la migrazione dei sistemi nel cloud;
- maggiore esternalizzazione dei servizi informatici.

Dal 2019 al 2021 il numero di incidenti significativi[1] a danno delle istituzioni, degli organi e delle agenzie dell'Unione, perpetrati da attori APT ("*advanced persistent threat*", "minacce mirate e persistenti"), è aumentato drasticamente. La prima metà del 2021 ha registrato un numero di incidenti significativi equivalente a quello dell'intero 2020. Ciò trova riscontro anche nel numero di immagini forensi (*snapshot* del contenuto dei sistemi o dispositivi colpiti) che il CERT-UE ha analizzato nel 2020, che sono triplicate rispetto al 2019, mentre il numero di incidenti significativi è più che decuplicato dal 2018.

Nel 2020 il comitato direttivo del CERT-UE ha stabilito un nuovo obiettivo strategico per tale centro allo scopo di garantire un livello esauriente di ciberdifesa per tutte le istituzioni, gli organi e le agenzie, di adeguata ampiezza e profondità e con un continuo adattamento alle minacce attuali o incombenti, compresi gli attacchi contro i dispositivi mobili, gli ambienti cloud e i dispositivi dell'internet degli oggetti.

A complemento dell'analisi delle minacce svolta dal CERT-UE, la Commissione ha proceduto a una valutazione del funzionamento della cibersicurezza in 20 istituzioni, organi e agenzie dell'Unione. Questo ha permesso di tracciare una panoramica delle pratiche di cibersicurezza

[1] Il termine "incidente significativo" indica qualsiasi incidente, salvo se presenta un impatto limitato ed è probabile che sia già adeguatamente compreso in termini di metodo o tecnologia.

vigenti, e delle capacità di gestione della cibersicurezza, con il riferimento esterno di una serie di controlli tecnici di sicurezza.

La valutazione si è basata su questionari ai quali tali istituzioni, organi e agenzie hanno risposto, su dati pubblici e su dati comunicati direttamente da tali soggetti. Essa fornisce conoscenze sufficienti sulla situazione attuale per poter concludere quanto segue:

- la maturità della cibersicurezza, la dimensione delle infrastrutture informatiche e i livelli di capacità variano considerevolmente fra le istituzioni, gli organi e le agenzie dell'Unione che sono stati oggetto della valutazione;
- benché molte istituzioni, organi e agenzie dell'Unione dispongano in generale di capacità di rilevamento e risposta mature, le loro capacità di governance in materia di cibersicurezza mostrano livelli diversi di gestione integrata dei rischi;
- benché le istituzioni, gli organi e le agenzie dell'Unione che sono stati oggetto della valutazione dispongano in generale di quadri di cibersicurezza (strategia, politica, e una base di norme) ben consolidati nei settori chiave di cibersicurezza elencati nell'allegato I del regolamento, in alcune istituzioni, organi e agenzie dell'Unione si constata invece una mancanza di maturità nella gestione della continuità operativa, nell'osservanza delle disposizioni, nell'audit e nelle attività di miglioramento continuo;
- risulta che nelle istituzioni, negli organi e nelle agenzie dell'Unione che sono stati oggetto della valutazione le misure tecniche considerate migliori pratiche sono applicate in modo disomogeneo.

In sintesi, l'analisi delle 20 istituzioni, organi e agenzie dell'Unione mostra un ampio spettro di diversità nella loro governance, igiene informatica, capacità generale e maturità. Pertanto, chiedere a tutte le istituzioni, tutti gli organi e tutte le agenzie dell'Unione di attuare una base di riferimento di misure di cibersicurezza è determinante per affrontare tale disparità di maturità e portare tutti questi soggetti a un livello comune elevato di cibersicurezza.

Nessuna normativa dell'Unione si è finora concentrata sula cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione, e ha affrontato in modo esaustivo il panorama delle minacce alla cibersicurezza e i rischi informatici emergenti derivanti dalla digitalizzazione.

- **Consultazioni dei portatori di interessi**

La Commissione ha consultato portatori di interessi presso l'insieme delle istituzioni, degli organi e delle agenzie dell'Unione come pure rappresentanti degli Stati membri al Consiglio e portatori di interessi presso il Parlamento europeo. Il 25 giugno 2021, rappresentanti degli Stati membri e portatori di interessi rilevanti delle istituzioni, organi e agenzie dell'Unione hanno partecipato a un seminario organizzato dalla Commissione per discutere il contenuto della futura proposta di regolamento.

- **Valutazione d'impatto**

La presente proposta avrà un impatto sulle istituzioni, sugli organi e sulle agenzie dell'Unione. Poiché non si applica agli Stati membri, non è necessaria una specifica valutazione d'impatto.

- **Diritti fondamentali**

L'Unione europea si impegna a garantire standard elevati in materia di tutela dei diritti fondamentali. Ogni condivisione di informazione in base al presente regolamento verrebbe attuata in ambienti sicuri nel pieno rispetto del diritto alla protezione dei dati di carattere personale sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e

della pertinente normativa in materia di protezione dei dati, nello specifico il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

4. INCIDENZA SUL BILANCIO

Da parametri di riferimento del mercato e da studi effettuati[2] emerge che la spesa diretta per la cibersicurezza ha registrato variazioni fra il 4 e il 7 % della spesa aggregata per l'informatica dei soggetti in questione. Tuttavia, l'analisi delle minacce intrapresa dal CERT-UE a sostegno della presente proposta legislativa indica che gli organismi internazionali e le organizzazioni politiche corrono rischi accresciuti, e che pertanto un livello del 10 % della spesa informatica per la cibersicurezza sembrerebbe un obiettivo più adeguato. Il costo esatto di tali sforzi non può essere determinato a causa della mancanza di informazioni dettagliate sulla spesa informatica delle istituzioni, degli organi e delle agenzie dell'Unione e la quota rilevante della spesa per la cibersicurezza.

Se è probabile, quindi, che molte istituzioni, organi e agenzie dell'Unione stanzino meno in cibersicurezza di quanto dovrebbero, il presente regolamento non causerà di per sé un aumento in tale spesa. Anche in assenza del regolamento, ciascun soggetto dovrebbe garantire un livello di cibersicurezza adeguato. Il regolamento porta avanti la precedente cooperazione nel comitato direttivo del CERT-UE e formalizza un livello di scambio di informazioni oggi già in parte esistente. Come indicato in dettaglio nella scheda finanziaria legislativa, il CERT-UE avrà bisogno di risorse aggiuntive per svolgere il suo ruolo più ampio, e tali risorse dovrebbero essere riassegnate dalle istituzioni, organi e agenzie dell'Unione che beneficiano dei suoi servizi.

5. ALTRI ELEMENTI

- **Modalità di attuazione, monitoraggio, valutazione e informazione**

Il comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board*, IICB), coadiuvato dal CERT-UE, dovrebbe esaminare il funzionamento del presente regolamento, effettuare valutazioni e presentare una relazione con le proprie conclusioni alla Commissione. La Commissione dovrebbe garantire la comunicazione periodica di informazioni al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni.

Il CERT-UE può elaborare una proposta di documento di orientamento o di raccomandazione, che l'IICB può scegliere di adottare. Un documento di orientamento è un documento di avviso destinato a tutte le istituzioni, organi e agenzie dell'Unione o a una parte di essi, mentre una raccomandazione è rivolta a singole istituzioni, singoli organi e singole agenzie dell'Unione. Un invito a intervenire è un documento di avviso del CERT-UE che descrive le misure di sicurezza urgenti che le istituzioni, gli organi e le agenzie dell'Unione sono esortati ad adottare entro un termine stabilito.

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

Disposizioni generali

[2] Fonte: Gartner, *"Identifying the Real Information Security Budget"* (2016). Ciò si aggiunge alla spesa indiretta per la sicurezza informatica, come quella per la sicurezza delle reti (*firewall*, antivirus), e le responsabilità del proprietario del sistema, come la valutazione dei rischi e l'attuazione dei controlli di sicurezza. Un articolo del 2020 colloca la spesa per la cibersicurezza negli istituti finanziari al 10-11 % della spesa informatica. Fonte: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Il regolamento stabilisce misure volte a garantire un livello comune elevato di cibersicurezza, e si applica alle istituzioni, organi e agenzie dell'Unione per consentire loro di svolgere le loro rispettive missioni in modo aperto, efficace e indipendente (articoli da 1 a 3 e da 23 a 25).

Misure per un livello comune elevato di cibersicurezza

Le istituzioni, gli organi e le agenzie dell'Unione sono tenuti a stabilire un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza che garantisca una gestione efficace e prudente di tutti i rischi per la cibersicurezza. Le istituzioni, gli organi e le agenzie adottano inoltre una base di riferimento per la cibersicurezza per affrontare i rischi individuati nell'ambito del quadro sopra indicato, svolgono valutazioni di maturità della cibersicurezza e adottano un piano di cibersicurezza (articoli da 4 a 8).

Comitato interistituzionale per la cibersicurezza

È istituito un comitato interistituzionale per la cibersicurezza, che avrà il compito di monitorare l'attuazione del presente regolamento da parte delle istituzioni, degli organi e delle agenzie dell'Unione, come pure di vigilare sull'attuazione delle priorità e degli obiettivi generali da parte del CERT-UE ed imprimere a tale centro una direzione strategica (articoli da 9 a 11).

CERT-UE

Il CERT-UE contribuirà alla sicurezza dell'ambiente informatico di tutte le istituzioni, organi e agenzie dell'Unione fornendo loro consulenza, sostenendoli nella prevenzione, nel rilevamento, nell'attenuazione degli incidenti e nella risposta agli stessi, e fungendo per tali soggetti da piattaforma per lo scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti (articoli da 12 a 17).

Cooperazione e obblighi di segnalazione

Il regolamento garantisce la cooperazione e lo scambio di informazioni fra il CERT-UE e le istituzioni, gli organi e le agenzie dell'Unione per sviluppare fiducia e fidatezza. A tal fine il CERT-UE può chiedere alle istituzioni, agli organi e alle agenzie dell'Unione di fornirgli informazioni rilevanti, e può, senza il consenso dell'utente interessato, scambiare informazioni specifiche su un incidente con le istituzioni, gli organi e le agenzie dell'Unione per facilitare il rilevamento di minacce informatiche o incidenti analoghi. Il CERT-UE può scambiare informazioni specifiche su un incidente che rivelino l'identità del bersaglio dell'incidente di cibersicurezza solo con il consenso dell'utente interessato.

In particolare, tutte le istituzioni, organi e agenzie dell'Unione notificano al CERT-UE le minacce informatiche significative, le vulnerabilità significative e gli incidenti significativi, senza indebito ritardo e in ogni caso entro 24 ore da quando ne sono venuti a conoscenza (articoli da 18 a 22).

2022/0085 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 298,

visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 106 bis,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Nell'era digitale, le tecnologie dell'informazione e della comunicazione sono fondamentali per un'amministrazione dell'Unione aperta, efficace ed indipendente. L'evoluzione della tecnologia e la maggiore complessità e interconnessione dei sistemi digitali amplificano i rischi per la cibersicurezza rendendo l'amministrazione dell'Unione più vulnerabile alle minacce e agli incidenti informatici, cosa che in ultima analisi rappresenta un pericolo per la continuità operativa dell'amministrazione e per la sua capacità di protezione dei propri dati. Se il maggior ricorso ai servizi cloud, l'uso massiccio delle tecnologie dell'informazione, l'elevata digitalizzazione, il lavoro a distanza, l'evoluzione delle tecnologie e la connettività sono oggi caratteristiche fondamentali di tutte le attività dei soggetti amministrativi dell'Unione, la resilienza digitale non è ancora sufficientemente integrata.

(2) Il panorama delle minacce informatiche che pesano sulle istituzioni, sugli organi e sulle agenzie dell'Unione è in costante divenire. Gli autori delle minacce impiegano tattiche, tecniche e procedure in continua evoluzione, mentre i moventi più usuali per questi attacchi cambiano di poco, dal furto di importanti informazioni riservate al profitto finanziario, alla manipolazione dell'opinione pubblica o l'indebolimento delle infrastrutture digitali. Il ritmo di perpetrazione degli attacchi informatici continua a intensificarsi, con campagne sempre più sofisticate e automatizzate che prendono di mira le superfici di attacco esposte, che continuano ad ampliarsi, sfruttando rapidamente le vulnerabilità.

(3) Gli ambienti informatici delle istituzioni, degli organi e delle agenzie dell'Unione sono interdipendenti, utilizzano flussi di dati integrati, e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un'istituzione, un organo o un'agenzia dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata sulle altre istituzioni, sugli altri organi o sulle altre agenzie dell'Unione. Alcuni ambienti informatici delle istituzioni, degli organi e delle agenzie dell'Unione sono inoltre connessi con gli ambienti informatici degli Stati

membri, e un incidente in un soggetto dell'Unione può quindi rappresentare un rischio per la cibersicurezza degli ambienti informatici degli Stati membri e viceversa.

(4) Le istituzioni, gli organi e le agenzie dell'Unione sono obiettivi interessanti, che si trovano a dover affrontare sia autori di minacce molto esperti e dotati di risorse adeguate, sia altri tipi di minacce. Al tempo stesso, fra tali soggetti dell'Unione, il livello e la maturità della ciberresilienza e la capacità di individuare e contrastare attività informatiche dolose varia in modo significativo. Ai fini del funzionamento dell'amministrazione europea è quindi necessario che le istituzioni, gli organi e le agenzie dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso una base di riferimento per la cibersicurezza (una serie di norme minime alle quali i sistemi informatici e di rete e i relativi operatori e utenti devono essere conformi al fine di ridurre al minimo i rischi per la cibersicurezza), lo scambio di informazioni e la collaborazione.

(5) La direttiva [proposta NIS 2] relativa a misure per un livello comune elevato di cibersicurezza nell'Unione è volta a migliorare ulteriormente le capacità di resilienza in termini di cibersicurezza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità e degli organi nazionali competenti così come dell'Unione nel suo complesso. È pertanto necessario che le istituzioni, gli organi e le agenzie dell'Unione agiscano in tal senso garantendo norme che siano coerenti con la direttiva [proposta NIS 2] e che rispecchino il suo livello di ambizione.

(6) Per raggiungere un livello comune elevato di cibersicurezza, è necessario che ogni istituzione, organo e agenzia dell'Unione stabilisca un quadro interno di gestione, governance e controllo dei rischi per la cibersicurezza, che garantisca una gestione efficace e prudente di tutti i rischi per la cibersicurezza, e tenga conto della continuità operativa e della gestione delle crisi.

(7) Le differenze esistenti fra le istituzioni, gli organi e le agenzie dell'Unione richiedono flessibilità nell'attuazione, poiché un approccio unico non sarà adatto a tutti. Le misure per un livello comune elevato di cibersicurezza non dovrebbero comportare alcun obbligo che interferisca direttamente con l'esercizio delle missioni delle istituzioni, degli organi e delle agenzie dell'Unione o che ne intacchi l'autonomia istituzionale. Tali istituzioni, organi e agenzie dovrebbero quindi istituire i propri quadri di gestione, governance e controllo dei rischi per la cibersicurezza, e dovrebbero adottare le proprie basi di riferimento e i propri piani di cibersicurezza.

(8) Per evitare di imporre un onere finanziario e amministrativo sproporzionato alle istituzioni, agli organi e alle agenzie dell'Unione, gli obblighi di gestione dei rischi per la cibersicurezza dovrebbero essere proporzionati al rischio corso dal sistema informatico e di rete interessato, tenendo conto delle misure più avanzate nel settore. Ogni istituzione, organo e agenzia dell'Unione dovrebbe mirare a stanziare un'adeguata percentuale del suo bilancio informatico per migliorare il livello di cibersicurezza; a lungo termine dovrebbe essere perseguito un obiettivo dell'ordine del 10 %.

(9) Un livello comune elevato di cibersicurezza richiede che tale aspetto sia soggetto alla sorveglianza del livello di dirigenza più elevato di ogni istituzione, organo e agenzia dell'Unione, che dovrebbe approvare un'apposita base di riferimento che consideri i rischi individuati nell'ambito del quadro che ogni istituzione, organo e agenzia deve stabilire. Occuparsi della cultura della cibersicurezza, ossia della pratica quotidiana della cibersicurezza, è parte integrante di una base di riferimento per la cibersicurezza in tutte le istituzioni, tutti gli organi e tutte le agenzie dell'Unione.

(10) Le istituzioni, gli organi e le agenzie dell'Unione dovrebbero valutare i rischi legati alle relazioni con i fornitori e i prestatori di servizi, compresi i prestatori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti, e dovrebbero adottare misure adeguate per affrontarli. Tali misure dovrebbero far parte della base di riferimento per la cibersicurezza e dovrebbero essere ulteriormente specificate in documenti di orientamento o raccomandazioni emanati dal CERT-UE. Nel definire le misure e gli orientamenti dovrebbero essere prese in debita considerazione le normative e politiche rilevanti dell'UE, comprese le valutazioni dei rischi e le raccomandazioni emanate dal gruppo di cooperazione NIS, come la valutazione dei rischi coordinata a livello dell'UE e il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G. Potrebbe essere inoltre richiesta la certificazione di prodotti, servizi e processi TIC nell'ambito di specifici sistemi di certificazione della cibersicurezza adottati conformemente all'articolo 49 del regolamento (UE) 2019/881,

(11) Nel maggio 2011 i segretari generali delle istituzioni e degli organi dell'Unione hanno deciso di costituire un gruppo per la preconfigurazione di una squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (di seguito "CERT-UE") posta sotto la supervisione di un comitato direttivo interistituzionale. Nel luglio 2012 i segretari generali hanno confermato le modalità pratiche e convenuto di mantenere il CERT-UE quale entità permanente per continuare a contribuire a migliorare il livello generale di sicurezza informatica delle istituzioni, degli organi e delle agenzie dell'Unione come esempio di cooperazione interistituzionale visibile in materia di cibersicurezza. Nel settembre 2012 il CERT-UE è stato istituito come task force della Commissione europea con un mandato interistituzionale. Nel dicembre 2017 le istituzioni e gli organi dell'Unione hanno concluso un accordo interistituzionale sull'organizzazione e il funzionamento del CERT-UE[3]. Tale accordo dovrebbe continuare ad evolversi per sostenere l'attuazione del presente regolamento.

(12) Il CERT-UE dovrebbe essere rinominato da "squadra di pronto intervento informatico" in "centro per la cibersicurezza" delle istituzioni, degli organi e delle agenzie dell'Unione, in linea con gli sviluppi negli Stati membri e a livello globale che vedono molti CERT-UE ribattezzati come "centri per la cibersicurezza", ma dovrebbe mantenere l'abbreviazione CERT-UE ai fini del riconoscimento del nome.

(13) Molti attacchi informatici fanno parte di campagne più ampie rivolte contro gruppi di istituzioni, organi e agenzie dell'Unione o comunità di interesse che comprendono le istituzioni, gli organi e le agenzie dell'Unione. Per consentire l'adozione di misure proattive di rilevamento, risposta agli incidenti o attenuazione, le istituzioni, gli organi e le agenzie dell'Unione dovrebbero notificare al CERT-UE le minacce informatiche significative, le vulnerabilità significative e gli incidenti significativi e dovrebbero condividere gli adeguati dettagli tecnici che consentano di rilevare od attenuare e di rispondere a minacce informatiche, vulnerabilità e incidenti analoghi in altre istituzioni, in altri organi e in altre agenzie dell'Unione.. Seguendo un approccio uguale a quello previsto nella direttiva [proposta NIS 2], qualora vengano a conoscenza di un incidente significativo, i soggetti in questione dovrebbero essere tenuti a presentare una notifica iniziale al CERT-UE entro 24 ore. Un tale scambio di informazioni dovrebbe consentire al CERT-UE di diffondere le informazioni alle altre istituzioni, agli altri organi e alle altre agenzie dell'Unione come pure agli omologhi

[3] GU C 12 del 13.1.2018, pag. 1.

rilevanti, per aiutare a proteggere gli ambienti informatici dell'Unione e quelli degli omologhi dell'Unione contro incidenti, minacce e vulnerabilità analoghi.

(14) Oltre a conferire maggiori compiti e un ruolo più ampio al CERT-UE, è opportuno istituire un comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board*, IICB), che dovrebbe contribuire all'instaurarsi di un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione monitorando l'attuazione del presente regolamento da parte di tali soggetti, vigilando sull'attuazione delle priorità e degli obiettivi generali da parte del CERT-UE, e imprimendo a tale centro una direzione strategica. L'IICB dovrebbe garantire la rappresentanza delle istituzioni e includere rappresentanti delle agenzie e degli organi attraverso la rete delle agenzie dell'Unione.

(15) Il CERT-UE dovrebbe sostenere l'attuazione delle misure per un livello comune elevato di cibersicurezza proponendo all'IICB documenti di orientamento e raccomandazioni ed emanando inviti a intervenire. Tali documenti di orientamento e raccomandazioni dovrebbero essere approvati dall'IICB. Ove necessario, il CERT-UE dovrebbe emanare inviti a intervenire che descrivono le misure di sicurezza urgenti che le istituzioni, gli organi e le agenzie dell'Unione sono esortati ad adottare entro un termine stabilito.

(16) L'IICB dovrebbe controllare l'osservanza del presente regolamento come pure il seguito dato ai documenti di orientamento e alle raccomandazioni, e agli inviti a intervenire emanati dal CERT-UE. L'IICB dovrebbe essere coadiuvato sulle questioni tecniche da gruppi di consulenza tecnica composti come da esso ritenuto utile, che dovrebbero lavorare in stretta collaborazione con il CERT-UE, con le istituzioni, gli organi e le agenzie dell'Unione e altri portatori di interessi a seconda delle necessità. Se del caso l'IICB dovrebbe emanare avvertimenti non vincolanti e raccomandare audit.

(17) Il CERT-UE dovrebbe avere la missione di contribuire alla sicurezza dell'ambiente informatico di tutte le istituzioni, di tutti gli organi e di tutte le agenzie dell'Unione. Il CERT-UE dovrebbe fungere da equivalente del coordinatore designato per le istituzioni, gli organi e le agenzie dell'Unione ai fini della divulgazione coordinata delle vulnerabilità al registro europeo delle vulnerabilità di cui all'articolo 6 della direttiva [proposta NIS 2].

(18) Nel 2020 il comitato direttivo del CERT-UE ha stabilito un nuovo obiettivo strategico per tale centro allo scopo di garantire un livello esauriente di ciberdifesa per tutte le istituzioni, gli organi e le agenzie dell'Unione, di adeguata ampiezza e profondità e con un continuo adattamento alle minacce attuali o incombenti, compresi gli attacchi contro i dispositivi mobili, gli ambienti cloud e i dispositivi dell'internet degli oggetti. L'obiettivo strategico include anche i centri operativi di sicurezza (SOC) ad ampio raggio di attività che controllano le reti, e il monitoraggio 24 ore al giorno, 7 giorni su 7, delle minacce di gravità elevata. Per quanto riguarda le istituzioni, gli organi e le agenzie dell'Unione di maggiori dimensioni, il CERT-UE dovrebbe sostenerne le équipe di sicurezza informatica, anche con un monitoraggio di prima linea 24 ore al giorno, 7 giorni su 7. Per quanto riguarda le istituzioni, gli organi e le agenzie dell'Unione di dimensioni più piccole e medie, il CERT-UE dovrebbe fornire l'insieme dei suoi servizi.

(19) Il CERT-UE dovrebbe inoltre svolgere il ruolo ad esso assegnato nella direttiva [proposta NIS 2] per quanto riguarda la cooperazione e lo scambio di informazioni con la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente

(CSIRT). Inoltre, per quanto riguarda la risposta, in linea con la raccomandazione (EU) 2017/1584 della Commissione[4] il CERT-UE dovrebbe garantire la cooperazione e il coordinamento con i portatori di interessi. Per contribuire a un livello comune elevato di cibersicurezza nell'Unione, il CERT-UE dovrebbe condividere con gli omologhi nazionali informazioni specifiche sugli incidenti. Il CERT-UE dovrebbe inoltre collaborare con altri omologhi pubblici e privati, anche in seno alla NATO, previa approvazione da parte dell'IICB.

(20) Nel sostenere la cibersicurezza operativa, il CERT-UE dovrebbe avvalersi delle competenze disponibili dell'Agenzia dell'Unione europea per la cibersicurezza attraverso una cooperazione strutturata di cui al regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[5]. Se del caso, dovrebbero essere conclusi appositi accordi tra i due soggetti per definire l'attuazione pratica di tale cooperazione ed evitare la duplicazione delle attività. Il CERT-UE dovrebbe cooperare con l'Agenzia dell'Unione europea per la cibersicurezza per quanto riguarda l'analisi delle minacce e dovrebbe condividere periodicamente con l'Agenzia la sua relazione sul panorama delle minacce.

(21) A sostegno dell'unità congiunta per il ciberspazio, istituita conformemente alla raccomandazione della Commissione del 23 giugno 2021[6], il CERT-UE dovrebbe cooperare e scambiare informazioni con i portatori di interessi per promuovere la cooperazione operativa e consentire alle reti esistenti di realizzare appieno il loro potenziale di protezione dell'Unione.

(22) Tutti i trattamenti di dati personali effettuati a norma del presente regolamento devono essere conformi alla legislazione in materia di protezione dei dati, compreso il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[7].

(23) Il trattamento delle informazioni da parte del CERT-UE e delle istituzioni, organi e agenzie dell'Unione dovrebbe essere in linea con le norme stabilite nel regolamento [proposta di regolamento sulla sicurezza delle informazioni]. Per garantire il coordinamento sulle questioni di sicurezza, ogni contatto con il CERT-UE avviato o sollecitato dai servizi nazionali di sicurezza e di intelligence dovrebbe essere comunicato senza indebito ritardo alla direzione "Sicurezza" della Commissione e al presidente dell'IICB

(24) Poiché i servizi e i compiti del CERT-UE sono svolti nell'interesse di tutte le istituzioni, organi e agenzie dell'Unione, ogni istituzione, organo e agenzia dell'Unione che sostenga spese informatiche dovrebbe contribuire con una quota equa a tali servizi e compiti. Tali contributi non pregiudicano l'autonomia di bilancio delle istituzioni, organi e agenzie dell'Unione.

---

4 Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

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

6 Raccomandazione C(2021) 4520 della Commissione, del 23 giugno 2021, sull'istituzione di un'unità congiunta per il ciberspazio.

7 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).

(25) L'IICB, coadiuvato dal CERT-UE, dovrebbe esaminare e valutare l'attuazione del presente regolamento e riferire le proprie conclusioni alla Commissione. Su tale base la Commissione dovrebbe riferire al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I
DISPOSIZIONI GENERALI

Articolo 1
Oggetto

Il presente regolamento stabilisce:

(a) l'obbligo, per le istituzioni, gli organi e le agenzie dell'Unione, di stabilire un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza;

(b) l'obbligo, per le istituzioni, gli organi e le agenzie dell'Unione, di gestione e di segnalazione dei rischi per la cibersicurezza;

(c) norme riguardanti l'organizzazione e il funzionamento del centro per la cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE) e l'organizzazione e il funzionamento del comitato interistituzionale per la cibersicurezza.

Articolo 2
Ambito di applicazione

Il presente regolamento si applica alla gestione, alla governance e al controllo dei rischi per la cibersicurezza da parte di tutte le istituzioni, tutti gli organi e tutte le agenzie dell'Unione, e all'organizzazione e al funzionamento del CERT-UE e del comitato interistituzionale per la cibersicurezza.

Articolo 3
Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) "istituzioni, organi e agenzie dell'Unione": le istituzioni, gli organi e le agenzie dell'Unione istituiti dal trattato sull'Unione europea, dal trattato sul funzionamento dell'Unione europea, dal trattato che istituisce la Comunità europea dell'energia atomica, oppure sulla base dei medesimi;

(2) "sistema informatico e di rete": il sistema informatico e di rete ai sensi dell'articolo 4, punto 1, della direttiva [proposta NIS 2];

(3) "sicurezza dei sistemi informatici e di rete": la sicurezza dei sistemi informatici e di rete ai sensi dell'articolo 4, punto 2, della direttiva [proposta NIS 2];

(4) "cibersicurezza": la cibersicurezza ai sensi dell'articolo 4, punto 3, della direttiva [proposta NIS 2];

(5) "livello di dirigenza più elevato": un dirigente, un organo di gestione o di coordinamento e sorveglianza al livello amministrativo più alto, tenuto conto dei

sistemi di governance ad alto livello di ogni istituzione, organo o agenzia dell'Unione;

(6) "incidente": un incidente ai sensi dell'articolo 4, punto 5, della direttiva [proposta NIS 2];

(7) "incidente significativo": qualsiasi incidente, salvo se presenta un impatto limitato ed è probabile che sia già adeguatamente compreso in termini di metodo o tecnologia;

(8) "attacco grave": qualsiasi incidente che richieda più risorse di quelle disponibili nell'istituzione, organo o agenzia interessati dell'Unione e presso il CERT-UE;

(9) "gestione degli incidenti": gestione degli incidenti ai sensi dell'articolo 4, punto 6, della direttiva [proposta NIS 2];

(10) "minaccia informatica": una minaccia informatica ai sensi dell'articolo 2, punto 8, del regolamento (UE) 2019/881;

(11) "minaccia informatica significativa": una minaccia informatica caratterizzata dall'intento, dalla possibilità e dalla capacità di causare un incidente significativo;

(12) "vulnerabilità": vulnerabilità ai sensi dell'articolo 4, punto 8, della direttiva [proposta NIS 2];

(13) "vulnerabilità significativa": una vulnerabilità che, se sfruttata, porterà probabilmente a un incidente significativo;

(14) "rischio per la cibersicurezza": ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza dei sistemi informatici e di rete;

(15) "unità congiunta per il ciberspazio": piattaforma virtuale e fisica per la cooperazione fra le diverse comunità di cibersicurezza nell'Unione, incentrata sulla cooperazione operativa e tecnica contro minacce e incidenti informatici transfrontalieri gravi ai sensi della raccomandazione della Commissione del 23 giugno 2021;

(16) "base di riferimento per la cibersicurezza": una serie di norme minime in materia di cibersicurezza alle quali i sistemi informatici e di rete e i relativi operatori e utenti devono essere conformi, al fine di ridurre al minimo i rischi per la cibersicurezza.

Capo II
MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA

Articolo 4
Gestione, governance e controllo dei rischi

1. Ogni istituzione, organo e agenzia dell'Unione stabilisce il proprio quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza ("il quadro") a sostegno della propria missione ed esercitando la propria autonomia istituzionale. Tali lavori sono soggetti alla vigilanza del livello di dirigenza più elevato dei rispettivi soggetti per garantire una gestione efficace e prudente di tutti i rischi per la cibersicurezza. Il quadro è predisposto entro il …. [15 mesi dopo l'entrata in vigore del presente regolamento].

2. Il quadro interessa la totalità dell'ambiente informatico dell'istituzione, dell'organo o dell'agenzia interessati, compresi ogni ambiente informatico in loco, le risorse e i servizi esternalizzati in ambienti di cloud computing od ospitati da terzi, i dispositivi

mobili, le reti interne, le reti professionali non connesse a internet e qualsiasi dispositivo connesso all'ambiente informatico. Il quadro tiene conto della continuità operativa e della gestione delle crisi e prende in considerazione la sicurezza della catena di approvvigionamento, come pure la gestione dei rischi umani che potrebbero avere ripercussioni sulla cibersicurezza dell'istituzione, organo o agenzia dell'Unione.

3. Il livello di dirigenza più elevato di ogni istituzione, organo e agenzia dell'Unione provvede a sorvegliare che la propria organizzazione rispetti gli obblighi relativi alla gestione, alla governance e al controllo dei rischi per la cibersicurezza, ferme restando le responsabilità formali degli altri livelli di dirigenza rispetto all'osservanza delle norme e alla gestione dei rischi nei rispettivi settori di competenza.

4. Ogni istituzione, organo e agenzia dell'Unione dispone di meccanismi efficaci per garantire che un'adeguata percentuale della dotazione di bilancio destinata alle tecnologie dell'informazione sia spesa per la cibersicurezza.

5. Ogni istituzione, organo e agenzia dell'Unione nomina un responsabile locale per la cibersicurezza o una funzione equivalente come proprio punto di contatto unico per tutti gli aspetti della cibersicurezza.

Articolo 5
Base di riferimento per la cibersicurezza

1. Il livello di dirigenza più elevato di ogni istituzione, organo e agenzia dell'Unione approva la base di riferimento per la cibersicurezza del rispettivo soggetto per affrontare i rischi individuati nell'ambito del quadro di cui all'articolo 4, paragrafo 1. Nel far ciò agisce a sostegno della sua missione e nell'esercizio della sua autonomia istituzionale. La base di riferimento per la cibersicurezza è predisposta entro il …. [18 mesi dopo l'entrata in vigore del presente regolamento] e riguarda i settori elencati nell'allegato I e le misure elencate nell'allegato II.

2. Gli alti dirigenti di ogni istituzione, organo e agenzia dell'Unione seguono periodicamente attività di formazione specifiche al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi e le pratiche di gestione in materia di cibersicurezza, e il loro impatto sulle attività dell'organizzazione.

Articolo 6
Valutazioni di maturità

Ogni istituzione, organo e agenzia dell'Unione svolge almeno ogni tre anni valutazioni di maturità della cibersicurezza, che comprendono tutti gli elementi del proprio ambiente informatico come descritto all'articolo 4, tenendo conto dei documenti di orientamento e delle raccomandazioni pertinenti adottati conformemente all'articolo 13.

Articolo 7
Piani di cibersicurezza

1. A seguito delle conclusioni tratte dalla valutazione di maturità e considerando le risorse e i rischi individuati ai sensi dell'articolo 4, il livello di dirigenza più elevato di ogni istituzione, organo e agenzia dell'Unione approva, senza indebito ritardo dopo l'istituzione del quadro di gestione, di governance e di controllo dei rischi e della base di riferimento per la cibersicurezza, un piano di cibersicurezza. Il piano è volto ad aumentare la cibersicurezza complessiva del soggetto interessato e contribuisce

così al conseguimento o al rafforzamento di un livello comune elevato di cibersicurezza in tutte le istituzioni, tutti gli organi e tutte le agenzie dell'Unione. A sostegno della missione del soggetto sulla base della sua autonomia istituzionale, il piano comprende come minimo i settori elencati nell'allegato I, le misure elencate nell'allegato II, come pure le misure riguardanti la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, come il monitoraggio della sicurezza e le pratiche di registrazione. Il piano è rivisto almeno ogni tre anni, a seguito delle valutazioni di maturità svolte ai sensi dell'articolo 6.

2. Il piano di cibersicurezza comprende i ruoli e le responsabilità del personale per la sua attuazione.

3. Il piano di cibersicurezza tiene conto di tutti i documenti di orientamento e di tutte le raccomandazioni applicabili emanati dal CERT-UE.

Articolo 8
Attuazione

1. Le istituzioni, gli organi e le agenzie dell'Unione sottopongono le valutazioni di maturità, una volta ultimate, al comitato interistituzionale per la cibersicurezza. Notificano inoltre allo stesso comitato interistituzionale per la cibersicurezza il completamento dei piani di cibersicurezza. Su richiesta del comitato, riferiscono in merito a specifici aspetti del presente capo.

2. I documenti orientativi e le raccomandazioni emanati conformemente all'articolo 13 sono d'ausilio all'attuazione delle disposizioni stabilite al presente capo.

Capo III
COMITATO INTERISTITUZIONALE PER LA CIBERSICUREZZA

Articolo 9
Comitato interistituzionale per la cibersicurezza

1. È istituito un comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board*, IICB).

2. L'IICB ha il compito di:

   (a) monitorare l'attuazione del presente regolamento da parte delle istituzioni, degli organi e delle agenzie dell'Unione;

   (b) vigilare sull'attuazione delle priorità e degli obiettivi generali da parte del CERT-UE ed imprimere a tale centro una direzione strategica.

3. L'IICB è composto da tre rappresentanti designati dalla rete delle agenzie dell'Unione (EUAN) su proposta del suo comitato consultivo TIC per difendere gli interessi delle agenzie e degli organi che gestiscono il proprio ambiente informatico, e da un rappresentante designato da ciascuno dei seguenti soggetti:

   (a) il Parlamento europeo;

   (b) il Consiglio dell'Unione europea;

   (c) la Commissione europea;

   (d) la Corte di giustizia dell'Unione europea;

   (e) la Banca centrale europea;

(f) la Corte dei conti europea;

(g) il Servizio europeo per l'azione esterna;

(h) il Comitato economico e sociale europeo;

(i) il Comitato europeo delle regioni;

(j) la Banca europea per gli investimenti;

(k) l'Agenzia dell'Unione europea per la cibersicurezza.

I membri possono farsi assistere da un supplente. Altri rappresentanti delle organizzazioni sopra elencate o di altre istituzioni, altri organi e altre agenzie dell'Unione possono essere invitati dal presidente ad assistere alle riunioni dell'IICB senza avere diritto di voto.

4. L'IICB adotta il proprio regolamento interno.

5. L'IICB designa un presidente, conformemente al proprio regolamento interno, tra i suoi membri per un periodo di quattro anni. Il supplente del presidente diventa membro a pieno titolo dell'IICB per la stessa durata.

6. L'IICB si riunisce su iniziativa del presidente, su richiesta del CERT-UE o su richiesta di uno dei membri.

7. Ciascun membro dell'IICB dispone di un voto. Le decisioni dell'IICB sono adottate a maggioranza semplice salvo disposizioni contrarie previste dal presente regolamento. Il presidente non partecipa al voto, tranne in caso di parità di voti, nel qual caso può esprimere il voto decisivo.

8. L'IICB può deliberare mediante una procedura scritta semplificata avviata conformemente al proprio regolamento interno. In base a tale procedura la pertinente decisione è considerata approvata entro il termine fissato dal presidente, salvo obiezioni da parte di uno dei membri.

9. Il direttore del CERT-UE, o il suo supplente, partecipa alle riunioni dell'IICB salvo se da questo diversamente deciso.

10. Le funzioni di segretariato dell'IICB sono espletate dalla Commissione.

11. I rappresentanti nominati dall'EUAN su proposta del comitato consultivo TIC trasmettono le decisioni dell'IICB alle imprese comuni e alle agenzie dell'Unione. Ogni agenzia e organo dell'Unione ha la facoltà di sottoporre al rappresentante o al presidente dell'IICB ogni questione che ritenga debba essere portata all'attenzione di tale comitato.

12. L'IICB può deliberare mediante una procedura scritta semplificata avviata dal presidente, in base alla quale la pertinente decisione è considerata approvata entro il termine fissato dal presidente, salvo obiezioni da parte di uno dei membri

13. L'IICB può nominare un comitato esecutivo che lo assista nel suo lavoro e può delegare a tale comitato alcuni dei suoi compiti e poteri. L'IICB stabilisce il regolamento interno del comitato esecutivo, compresi i suoi compiti e i suoi poteri, e il mandato dei suoi membri.

Articolo 10
Compiti dell'IICB

Nell'esercizio delle sue responsabilità l'IICB, in particolare:

(a) esamina le relazioni richieste al CERT-UE sullo stato di attuazione del presente regolamento da parte delle istituzioni, degli organi e delle agenzie dell'Unione;

(b) approva, sulla base di una proposta del direttore del CERT-UE, il programma di lavoro annuale del CERT-UE e ne monitora l'attuazione;

(c) approva, sulla base di una proposta del direttore del CERT-UE, il catalogo dei servizi offerti dal CERT-UE;

(d) approva, sulla base di una proposta presentata dal direttore del CERT-UE, la pianificazione finanziaria annuale delle entrate e delle spese, anche per il personale, per le attività del CERT-UE;

(e) approva, sulla base di una proposta del direttore del CERT-UE, le modalità degli accordi sul livello dei servizi;

(f) esamina e approva la relazione annuale elaborata dal direttore del CERT-UE riguardante le attività del CERT-UE, nonché la gestione dei fondi da parte di quest'ultimo;

(g) approva e monitora gli indicatori essenziali di prestazione per il CERT-UE definiti su proposta del direttore del CERT-UE;

(h) approva gli accordi di cooperazione, gli accordi sul livello dei servizi o i contratti tra il CERT-UE ed altri soggetti ai sensi dell'articolo 17;

(i) istituisce tutti i gruppi di consulenza tecnica necessari per assistere l'IICB nel suo operato, approva il loro mandato e ne designa i rispettivi presidenti.

Articolo 11
Osservanza delle disposizioni

L'IICB controlla che le istituzioni, gli organi e le agenzie dell'Unione attuino il presente regolamento e i documenti di orientamento, le raccomandazioni e gli inviti a intervenire adottati. Qualora constati che le istituzioni, gli organi o le agenzie dell'Unione non hanno applicato o attuato efficacemente il presente regolamento o i documenti di orientamento, le raccomandazioni e gli inviti a intervenire emanati ai sensi del presente regolamento l'IICB può, ferme restando le procedure interne dell'istituzione, dell'organo o dell'agenzia dell'Unione pertinente:

(a) emanare un avvertimento; ove necessario, in considerazione di un rischio perentorio per la cibersicurezza, i destinatari dell'avvertimento sono adeguatamente circoscritti;

(b) raccomandare lo svolgimento di un audit da parte di un servizio competente.

Capo IV
CERT-UE

Articolo 12
Missione e compiti del CERT-UE

1. La missione del CERT-UE, il centro autonomo per la cibersicurezza di tutte le istituzioni, gli organi e le agenzie dell'Unione, consiste nel contribuire alla sicurezza dell'ambiente informatico non riservato di tutti questi soggetti fornendo loro consulenza in materia di cibersicurezza, aiutandoli a prevenire, rilevare, attenuare gli incidenti e a rispondere agli stessi, e fungendo per tali soggetti da piattaforma per lo

scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti.

2. Il CERT-UE svolge i seguenti compiti per le istituzioni, gli organi e le agenzie dell'Unione:

   (a) li assiste nell'attuazione del presente regolamento e contribuisce al coordinamento della sua applicazione tramite le misure di cui all'articolo 13, paragrafo 1, o tramite relazioni ad hoc richieste dall'IICB;

   (b) li assiste con un pacchetto di servizi di cibersicurezza descritti nel proprio catalogo dei servizi ("servizi di base");

   (c) mantiene una rete di omologhi e partner a sostegno dei propri servizi, come indicato agli articoli 16 e 17;

   (d) richiama l'attenzione dell'IICB su ogni questione relativa all'attuazione del presente regolamento e all'attuazione dei documenti di orientamento, delle raccomandazioni e degli inviti a intervenire;

   (e) riferisce in merito alle minacce informatiche cui sono esposti le istituzioni, gli organi e le agenzie dell'Unione e contribuisce alla consapevolezza situazionale informatica dell'UE.

3. Il CERT-UE contribuisce all'unità congiunta per il ciberspazio, istituita conformemente alla raccomandazione della Commissione del 23 giugno 2021, anche nei seguenti settori:

   (a) preparazione, coordinamento in caso di incidente, scambio di informazioni e risposta alle crisi a livello tecnico relativamente a casi collegati alle istituzioni, agli organi e alle agenzie dell'Unione;

   (b) cooperazione operativa per quanto riguarda la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), anche per l'assistenza reciproca, e la più ampia comunità della cibersicurezza;

   (c) intelligence relativa alle minacce informatiche, compresa la consapevolezza situazionale;

   (d) ogni tematica che richieda le competenze tecniche in materia di cibersicurezza del CERT-UE.

4. Il CERT-UE avvia una cooperazione strutturata con l'Agenzia dell'Unione europea per la cibersicurezza in materia di sviluppo di capacità, cooperazione operativa e analisi strategiche a lungo termine delle minacce informatiche ai sensi del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio.

5. Il CERT-UE può prestare i seguenti servizi non descritti nel suo catalogo dei servizi ("servizi addebitabili"):

   (a) servizi a sostegno della cibersicurezza dell'ambiente informatico delle istituzioni, degli organi e delle agenzie dell'Unione, diversi da quelli di cui al paragrafo 2, forniti in base ad accordi sul livello dei servizi e compatibilmente con le risorse disponibili;

   (b) servizi a sostegno di operazioni o progetti di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione, diversi da quelli volti a proteggere il loro ambiente informatico, forniti in base ad accordi scritti e previa approvazione dell'IICB;

(c) servizi a sostegno della sicurezza dell'ambiente informatico di organizzazioni diverse dalle istituzioni, dagli organi e dalle agenzie dell'Unione e che cooperano strettamente con tali istituzioni, organi e agenzie, ad esempio perché investite di compiti o responsabilità ai sensi del diritto dell'Unione, forniti in base ad accordi scritti e previa approvazione dell'IICB.

6. Il CERT-UE può organizzare esercitazioni di cibersicurezza o raccomandare la partecipazione alle esercitazioni esistenti, in stretta cooperazione con l'Agenzia dell'Unione europea per la cibersicurezza se del caso, per verificare il livello di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione.

7. Il CERT-UE può fornire assistenza alle istituzioni, agli organi e alle agenzie dell'Unione in caso di incidenti in ambienti informatici riservati se l'utente interessato lo richiede esplicitamente.

Articolo 13

Documenti di orientamento, raccomandazioni e inviti a intervenire

1. Il CERT-UE contribuisce all'attuazione del presente regolamento emanando:

(a) inviti a intervenire che descrivono le misure di sicurezza urgenti che le istituzioni, gli organi e le agenzie dell'Unione sono esortate ad adottare entro un termine stabilito;

(b) proposte all'IICB per documenti di orientamento destinati a tutte le istituzioni, a tutti gli organi e a tutte le agenzie dell'Unione o a una parte di essi;

(c) proposte all'IICB per raccomandazioni destinate a singole istituzioni, singoli organi e singole agenzie dell'Unione.

2. I documenti di orientamento e le raccomandazioni possono contenere:

(a) modalità, o miglioramenti, riguardanti la gestione dei rischi per la cibersicurezza e la base di riferimento per la cibersicurezza;

(b) modalità relative alle valutazioni di maturità e ai piani di cibersicurezza, e

(c) se del caso, disposizioni sull'utilizzo di una tecnologia, architettura e relative migliori pratiche comuni allo scopo di conseguire interoperabilità e norme comuni.ai sensi dell'articolo 4, punto 10, della direttiva [proposta NIS 2].

3. L'IICB può adottare i documenti di orientamento o le raccomandazioni proposti dal CERT-UE.

4. L'IICB può chiedere al CERT-UE di emanare, ritirare o modificare una proposta per documenti di orientamento o raccomandazioni, o un invito a intervenire.

Articolo 14
Direttore del CERT-UE

Il direttore del CERT-UE presenta periodicamente all'IICB e al presidente di tale comitato relazioni riguardanti le prestazioni del CERT-UE, la pianificazione finanziaria, le entrate, l'esecuzione del bilancio, gli accordi sul livello dei servizi e gli accordi scritti conclusi, la cooperazione con omologhi e partner e le missioni effettuate dal personale, comprese le relazioni di cui all'articolo 10, paragrafo 1.

Articolo 15
Questioni finanziarie e relative al personale

1. La Commissione, dopo aver ottenuto l'approvazione unanime dell'IICB, nomina il direttore del CERT-UE. L'IICB è consultato in tutte le fasi della procedura di nomina del direttore del CERT-UE, in particolare nell'ambito della redazione degli avvisi di posto vacante, dell'esame delle candidature e della designazione delle commissioni giudicatrici in relazione a tale incarico.
2. Per l'applicazione delle procedure amministrative e finanziarie, il direttore del CERT-UE agisce sotto l'autorità della Commissione.
3. I compiti e le attività del CERT-UE, compresi i servizi da esso prestati ai sensi dell'articolo 12, paragrafi 2, 3, 4, e 6, e dell'articolo 13, paragrafo 1, alle istituzioni, agli organi e alle agenzie dell'Unione rientranti nella rubrica del quadro finanziario pluriennale relativa alla pubblica amministrazione europea, sono finanziati tramite una linea distinta del bilancio della Commissione. I posti riservati al CERT-UE sono specificati in una nota a piè di pagina della tabella dell'organico della Commissione.
4. Le istituzioni, gli organi e le agenzie dell'Unione diversi da quelli di cui al paragrafo 3 forniscono un contributo finanziario annuale al CERT-UE per coprire i servizi da esso prestati ai sensi dello stesso paragrafo 3. I rispettivi contributi sono basati su orientamenti dati dall'IICB e concordati tra ciascun soggetto e il CERT-UE in accordi sul livello dei servizi. I contributi rappresentano una quota equa e proporzionata dei costi totali dei servizi forniti. Essi sono assegnati alla linea di bilancio distinta di cui al paragrafo 3 come entrate con destinazione specifica ai sensi dell'articolo 21, paragrafo 3, lettera c), del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio[8].
5. I costi dei compiti di cui all'articolo 12, paragrafo 5, sono a carico delle istituzioni, degli organi e delle agenzie dell'Unione che ricevono i servizi del CERT-UE. Le entrate sono destinate alle linee di bilancio che sostengono i costi.

Articolo 16
Cooperazione tra il CERT-UE e gli omologhi degli Stati membri

1. Il CERT-UE coopera e scambia informazioni con gli omologhi nazionali degli Stati membri, compresi i CERT, i centri nazionali per la cibersicurezza, gli CSIRT e i punti di contatto unici di cui all'articolo 8 della direttiva [proposta NIS 2] in merito

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

alle minacce informatiche, alle vulnerabilità e agli incidenti, alle possibili contromisure e in merito a tutte le questioni pertinenti per il miglioramento della protezione degli ambienti informatici delle istituzioni, degli organi e delle agenzie dell'Unione, anche tramite la rete di CSIRT di cui all'articolo 13 della direttiva [proposta NIS 2].

2. Il CERT-UE può, senza il consenso dell'utente interessato, scambiare informazioni specifiche su un incidente con gli omologhi nazionali degli Stati membri per facilitare il rilevamento di minacce informatiche o incidenti analoghi. Il CERT-UE può scambiare informazioni specifiche su un incidente che rivelino l'identità del bersaglio dell'incidente di cibersicurezza solo con il consenso dell'utente interessato.

Articolo 17
Cooperazione tra il CERT-UE ed omologhi di paesi terzi

1. Il CERT-UE può cooperare con omologhi di paesi terzi, compresi omologhi di settori specifici, riguardo a strumenti e metodi, quali tecniche, tattiche, procedure e migliori pratiche, nonché minacce informatiche e vulnerabilità. Per procedere a qualsiasi cooperazione con tali omologhi, anche in ambiti in cui questi collaborino con omologhi nazionali degli Stati membri, il CERT-UE chiede l'approvazione preventiva dell'IICB.

2. Il CERT-UE può cooperare con altri partner, quali soggetti commerciali, organizzazioni internazionali, enti nazionali non dell'Unione europea o singoli esperti, al fine di raccogliere informazioni su minacce informatiche generali e specifiche, vulnerabilità, nonché possibili contromisure. Per procedere a una più ampia cooperazione con tali partner, il CERT-UE chiede l'approvazione preventiva dell'IICB.

3. Il CERT-UE può, con il consenso dell'utente interessato da un incidente, fornire informazioni in merito all'incidente a partner che possono contribuire alla sua analisi.

Capo V
COOPERAZIONE E OBBLIGHI DI SEGNALAZIONE

Articolo 18
Trattamento delle informazioni

1. Il CERT-UE e le istituzioni, gli organi e le agenzie dell'Unione rispettano l'obbligo del segreto professionale ai sensi dell'articolo 339 del trattato sul funzionamento dell'Unione europea o di equivalenti quadri normativi applicabili.

2. Alle richieste di accesso del pubblico ai documenti detenuti dal CERT-UE si applicano le disposizioni del regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[9], compreso l'obbligo, previsto da tale regolamento, di consultare le altre istituzioni, gli altri organi e le altre agenzie dell'Unione qualora la domanda riguardi loro documenti.

[9] 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).

3. Il trattamento dei dati personali effettuato in virtù del presente regolamento è soggetto alle disposizioni del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

4. Il trattamento delle informazioni da parte del CERT-UE e delle istituzioni, degli organi e delle agenzie dell'Unione è in linea con le norme stabilite nella [proposta di regolamento sulla sicurezza delle informazioni].

5. Ogni contatto con il CERT-UE avviato o sollecitato dai servizi nazionali di sicurezza e di intelligence è comunicato senza indebito ritardo alla direzione "Sicurezza" della Commissione e al presidente dell'IICB.

Articolo 19
Obblighi di condivisione di informazioni

1. Per poter coordinare la gestione delle vulnerabilità e la risposta agli incidenti, il CERT-UE può chiedere alle istituzioni, agli organi e alle agenzie dell'UE di fornirgli informazioni, tratte dai loro rispettivi inventari dei sistemi informatici, che siano pertinenti per il sostegno al suo lavoro. L'istituzione, l'organo o l'agenzia cui è rivolta tale domanda trasmette senza indebito ritardo le informazioni richieste e ogni loro successivo aggiornamento.

2. Le istituzioni, gli organi e le agenzie dell'Unione, su richiesta del CERT-UE e senza indebito ritardo, forniscono a tale centro le informazioni digitali generate dall'uso dei dispositivi elettronici coinvolti nei loro rispettivi incidenti. Il CERT-UE può chiarire ulteriormente di quali tipi di informazioni digitali ha bisogno ai fini della consapevolezza situazionale e della risposta agli incidenti.

3. IL CERT-UE può scambiare informazioni specifiche su un incidente che rivelino l'identità dell'istituzione, dell'organo o dell'agenzia interessati dall'incidente solo con il consenso di tale soggetto. Il CERT-UE può scambiare informazioni specifiche su un incidente che rivelino l'identità del bersaglio dell'incidente di cibersicurezza solo con il consenso del soggetto interessato dall'incidente.

4. Gli obblighi di condivisione non comprendono le informazioni classificate UE ("ICUE") e le informazioni che un'istituzione, un organo o un'agenzia dell'Unione ha ricevuto da un servizio di sicurezza o di intelligence o da un'autorità di contrasto di uno Stato membro con l'esplicita condizione di non trasmetterle al CERT-UE.

Articolo 20
Obblighi di notifica

1. Tutte le istituzioni, tutti gli organi e tutte le agenzie dell'Unione presentano al CERT-UE una notifica iniziale delle minacce informatiche significative, delle vulnerabilità significative e degli incidenti significativi, senza indebito ritardo e in ogni caso entro 24 ore dopo esserne venuti a conoscenza.

   In casi debitamente giustificati e con l'accordo del CERT-UE, l'istituzione, l'organo o l'agenzia dell'Unione in questione può derogare alla scadenza di cui al paragrafo precedente.

2. Le istituzioni, gli organi e le agenzie dell'Unione notificano inoltre al CERT-UE, senza indebito ritardo, gli adeguati dettagli tecnici concernenti le minacce informatiche, le vulnerabilità e gli incidenti, che consentano l'adozione di misure di

rilevamento, risposta agli incidenti o attenuazione. La notifica include, se sono disponibili:

(a) gli indicatori di compromissione pertinenti;

(b) i meccanismi di rilevamento pertinenti;

(c) le potenziali conseguenze;

(d) le misure di attenuazione pertinenti.

3. Il CERT-UE trasmette mensilmente all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sulle minacce informatiche significative, sulle vulnerabilità significative e sugli incidenti significativi notificati conformemente al paragrafo 1.

4. L'IICB può emanare documenti di orientamento e raccomandazioni riguardanti le modalità e il contenuto della notifica. Il CERT-UE diffonde gli adeguati dettagli tecnici che consentano l'adozione di misure proattive di rilevamento, risposta agli incidenti o attenuazione da parte delle istituzioni, degli organi e delle agenzie dell'Unione.

5. Gli obblighi di notifica non comprendono le ICUE e le informazioni che un'istituzione, un organo o un'agenzia dell'Unione ha ricevuto da un servizio di sicurezza o di intelligence o da un'autorità di contrasto di uno Stato membro con l'esplicita condizione di non trasmetterle al CERT-UE.

Articolo 21

Coordinamento della risposta in caso di incidenti e cooperazione in caso di incidenti significativi

1. Fungendo da piattaforma per lo scambio di informazioni in materia di cibersicurezza e il coordinamento della risposta in caso di incidenti, il CERT-UE facilita la circolazione delle informazioni riguardo alle minacce informatiche, alle vulnerabilità e agli incidenti tra:

(e) le istituzioni, gli organi e le agenzie dell'Unione;

(f) gli omologhi di cui agli articoli 16 e 17.

2. Il CERT-UE facilita il coordinamento fra le istituzioni, gli organi e le agenzie dell'Unione in materia di risposta agli incidenti, anche tramite:

(g) il contributo a una comunicazione esterna coerente;

(h) l'assistenza reciproca;

(i) l'uso ottimale delle risorse operative;

(j) il coordinamento con altri meccanismi di risposta alle crisi a livello dell'Unione.

3. Il CERT-UE sostiene le istituzioni, gli organi e le agenzie dell'Unione per quanto riguarda la consapevolezza situazionale delle minacce informatiche, delle vulnerabilità e degli incidenti.

4. l'IICB emana orientamenti sul coordinamento della risposta in caso di incidenti e sulla cooperazione in caso di incidenti significativi. In caso di sospetta natura criminale di un incidente, il CERT-UE fornisce consulenza su come segnalare l'incidente alle autorità di contrasto.

Articolo 22
Attacco grave

1. Il CERT-UE coordina, fra le istituzioni, gli organi e le agenzie dell'Unione, le risposte agli attacchi gravi. Il CERT-UE tiene un inventario delle competenze tecniche che risulterebbero necessarie per la risposta agli incidenti in caso di attacchi di questo tipo.
2. Le istituzioni, gli organi e le agenzie dell'Unione contribuiscono all'inventario delle competenze tecniche fornendo un elenco annualmente aggiornato di esperti disponibili al loro interno, che specifichi le loro capacità tecniche.
3. Con l'accordo delle istituzioni, degli organi e delle agenzie dell'Unione interessati, il CERT-UE può anche rivolgersi agli esperti dell'elenco di cui al paragrafo 2 per contribuire alla risposta a un attacco grave in uno Stato membro, in linea con le procedure operative dell'unità congiunta per il ciberspazio.

Capo VI
DISPOSIZIONI FINALI

Articolo 23
Riassegnazione di bilancio iniziale

La Commissione propone la riassegnazione di personale e risorse finanziarie dalle istituzioni, dagli organi e dalle agenzie dell'Unione al proprio bilancio. La riassegnazione è effettiva contestualmente al primo bilancio adottato dopo l'entrata in vigore del presente regolamento.

Articolo 24
Riesame

1. L'IICB, coadiuvato dal CERT-UE, riferisce periodicamente alla Commissione in merito all'attuazione del presente regolamento. L'IICB può anche rivolgere raccomandazioni alla Commissione per proporre modifiche al presente regolamento.
2. La Commissione riferisce al Parlamento europeo e al Consiglio in merito all'attuazione del presente regolamento entro 48 mesi dalla sua entrata in vigore e successivamente ogni tre anni.
3. La Commissione valuta il funzionamento del presente regolamento e riferisce al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni trascorsi almeno cinque anni dalla data di entrata in vigore.

Articolo 25

Entrata in vigore

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

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

Fatto a Bruxelles, il

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

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. La proposta/iniziativa riguarda:

1.4. Obiettivi

1.4.1. Obiettivi generali

1.4.2. Obiettivi specifici

1.4.3. Risultati e incidenza previsti

1.4.4. Indicatori di prestazione

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

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

1.5.3. Insegnamenti tratti da esperienze analoghe

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

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

1.6. Durata e incidenza finanziaria della proposta/iniziativa

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

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

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

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

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

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

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, organi e organismi dell'Unione

1.2. Settore/settori interessati

Pubblica amministrazione europea

La proposta contiene misure che garantiscono un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione

1.3. La proposta/iniziativa riguarda:

☑una nuova azione

☐ una nuova azione a seguito di un progetto pilota/un'azione preparatoria[10]

☐ la proroga di un'azione esistente

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

1.4. Obiettivi

1.4.1. Obiettivi generali

– Istituire un quadro per garantire un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione

– Fornire una nuova base giuridica per il CERT-UE al fine di consolidarne mandato e finanziamenti.

1.4.2. Obiettivi specifici

(1) Fare obbligo alle istituzioni, organi e agenzie dell'Unione di istituire un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza

(2) Fare obbligo alle istituzioni, organi e agenzie dell'Unione di riferire in merito al loro quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza così come sugli incidenti di cibersicurezza.

(3) Stabilire le norme riguardanti l'organizzazione e il funzionamento del centro per la cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE) e l'organizzazione e il funzionamento del comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board*, IICB)

(4) Contribuire all'unità congiunta per il ciberspazio

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

1.4.3. Risultati e incidenza previsti

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

- Quadri interni di gestione, di governance e di controllo dei rischi per la cibersicurezza, basi di riferimento per la cibersicurezza, valutazioni di maturità periodiche e piani di cibersicurezza nelle istituzioni, organi e agenzie dell'Unione
- Miglioramento delle capacità di resilienza in termini di cibersicurezza e di risposta agli incidenti nelle istituzioni, organi e agenzie dell'Unione
- Modernizzazione del CERT-UE
- Contributo all'unità congiunta per il ciberspazio

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati.

- Quadri e basi di riferimento predisposti, valutazioni di maturità periodiche e piani di cibersicurezza svolti nelle istituzioni, organi e agenzie dell'Unione
- Miglioramenti nella gestione degli incidenti
- Aumento della consapevolezza dei rischi per la cibersicurezza a livello di alta dirigenza delle istituzioni, organi e agenzie dell'Unione
- Livellamento della spesa per la sicurezza delle TIC come percentuale della spesa complessiva per le TIC
- Forte leadership dell'IICB e del CERT-UE
- Aumento della condivisione delle informazioni tra le istituzioni, gli organi e le agenzie dell'Unione e con gli organismi e le parti interessate rilevanti nell'UE
- Aumento della cooperazione in materia di cibersicurezza con gli organismi e le parti interessate rilevanti nell'UE, attraverso il CERT-UE e l'ENISA

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa.

La proposta è volta ad aumentare il livello di ciberresilienza nelle istituzioni, organi e agenzie dell'Unione, a ridurre le disomogeneità nella resilienza fra tali soggetti, e a migliorare il livello di consapevolezza situazionale comune e di capacità collettiva di preparazione e risposta.

La proposta è pienamente coerente e in linea con altre iniziative affini, e in particolare con la proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 [proposta NIS 2].

La proposta è una parte essenziale della strategia dell'UE per l'Unione della sicurezza e della strategia dell'UE in materia di cibersicurezza per il decennio digitale.

Secondo il programma, la proposta di regolamento da parte della Commissione europea è per ottobre 2021, l'adozione del regolamento da parte del Parlamento europeo e del Consiglio è prevista nel 2022, e le disposizioni saranno applicabili dalla sua entrata in vigore. L'impatto finanziario e in termini di risorse umane delineato nella presente scheda finanziaria legislativa dovrebbe iniziare nel 2023. Un

periodo preparatorio è già iniziato nel 2021, ma le attività preparatorie del 2021 e del 2022 non rientrano nell'impatto finanziario della proposta.

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

Motivi dell'azione a livello europeo (ex ante)

Dal 2019 al 2021 il numero di incidenti significativi a danno delle istituzioni, degli organi e delle agenzie dell'Unione, perpetrati da attori di minacce mirate e persistenti, è aumentato drasticamente. La prima metà del 2021 ha registrato un numero di incidenti significativi equivalente a quello dell'intero 2020. Ciò trova riscontro anche nel numero di immagini forensi (snapshot del contenuto dei sistemi o dispositivi colpiti) che il CERT-UE ha analizzato nel 2020, che sono triplicate rispetto al 2019, mentre il numero di incidenti significativi è più che decuplicato dal 2018.

I livelli di maturità della cibersicurezza variano considerevolmente da un soggetto a un altro[11]. Il presente regolamento garantisce che tutte le istituzioni, organi e agenzie dell'Unione attueranno una base di riferimento per le misure di sicurezza e coopereranno fra di loro ai fini di un funzionamento aperto ed efficiente dell'amministrazione dell'Unione.

I sistemi da preservare rientrano nell'autonomia delle istituzioni, organi e agenzie dell'Unione e sono da essi gestiti; le azioni proposte non potrebbero essere predisposte dagli Stati membri.

1.5.3. Insegnamenti tratti da esperienze analoghe

La direttiva NIS è stata il primo strumento orizzontale del mercato interno volto a migliorare la resilienza di reti e sistemi nell'Unione rispetto ai rischi di cibersicurezza. Dalla sua entrata in vigore nel 2016 ha contribuito notevolmente a innalzare il livello comune di cibersicurezza tra gli Stati membri. La proposta di direttiva NIS 2 è volta a migliorare ulteriormente queste misure.

Il regolamento è volto a introdurre misure analoghe per le istituzioni, gli organi e le agenzie dell'Unione.

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

La proposta è coerente con il quadro finanziario pluriennale ed è una parte essenziale della strategia dell'UE per l'Unione della sicurezza come pure della strategia dell'UE in materia di cibersicurezza per il decennio digitale.

La proposta prevede l'applicazione di misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione, ed è in linea con la proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 [proposta NIS 2].

[11] Riferimento: [Relazione speciale della CCE sulla cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione].

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

La gestione dei compiti da parte del CERT-UE richiede profili specifici e comporta carichi di lavoro supplementari che non possono essere assorbiti senza un aumento delle risorse umane

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **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**

– L'incidenza finanziaria dovrebbe iniziare con il primo bilancio adottato dopo l'entrata in vigore del regolamento. Una riassegnazione di risorse dalle istituzioni e dai principali organi dell'Unione alla Commissione avrebbe luogo nel primo anno, considerato un anno di transizione; questa e altre (ri)assegnazioni di risorse avranno luogo nel quadro dei bilanci annuali. Se il regolamento è adottato nel 2022, l'esercizio finanziario 2023 sarà il periodo di transizione, e il 2024 sarà operativo a pieno regime.

1.7. Modalità di gestione previste[12]

☑ **Gestione diretta** a opera della Commissione e di ogni istituzione, organo e agenzia dell'Unione

– ☑ 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 i compiti di esecuzione del bilancio:

– ☐ a paesi terzi o a organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI 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;

– ☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V del TUE e indicate nel pertinente atto di base.

[12] Le spiegazioni dettagliate sulle modalità di gestione e i riferimenti al regolamento finanziario sono reperibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

Per l'applicazione delle procedure amministrative e finanziarie, il CERT-UE agisce sotto l'autorità della Commissione.

Risorse aggiuntive derivanti dal progetto di regolamento:

L'attuazione degli articoli 12 e 13 del progetto di regolamento porta a un catalogo di servizi ampliato con servizi di base supplementari. Col funzionamento a pieno regime, saranno necessarie le seguenti risorse aggiuntive (fino al termine del QFP, fine 2027): 21 ETP e 14,05 milioni di EUR.

La ripartizione delle risorse aggiuntive nell'ambito del bilancio fra i vari compiti è la seguente:

(a) per l'esecuzione dei compiti per le istituzioni, organi e agenzie dell'Unione specificati all'articolo 12, paragrafo 2, lettere a), b), c) ed e): 13,75 ETP e 11,275 milioni di EUR;

(b) per l'esecuzione dei compiti specificati all'articolo 12, paragrafo 3 (contributo all'unità congiunta per il ciberspazio): 2 ETP e 381 000 EUR;

(c) per l'esecuzione dei compiti specificati all'articolo 12, paragrafo 4 (cooperazione strutturata con l'ENISA): 0,25 ETP e 236 000 EUR;

(d) per l'esecuzione dei compiti specificati all'articolo 12, paragrafo 6 (esercitazioni di cibersicurezza): 0,25 ETP e 79 000 EUR;

(e) per l'esecuzione dei compiti specificati all'articolo 12, paragrafo 2, lettera d) e all'articolo 13 (analisi e relazioni sull'attuazione del regolamento, preparazione dei documenti di orientamento, delle raccomandazioni e degli inviti a intervenire): 3,75 ETP e 2,079 milioni di EUR.

(f) per l'esecuzione dei compiti di sostegno al segretariato del comitato interistituzionale per la cibersicurezza (IICB): 1 ETP.

Panoramica delle risorse attuali e transizione a pieno regime:

Nel settembre 2021 il CERT-UE ha operato con le seguenti risorse:

- posti permanenti e distaccati: 14 ETP;

- agenti contrattuali finanziati nel quadro di accordi sul livello dei servizi: 24 ETP;

- totale: 38 ETP.

Il bilancio del CERT-UE nel 2020 era il seguente: 250 000 EUR provenienti dal bilancio della Commissione e 3,5 milioni di EUR come entrate con destinazione specifica nel quadro di accordi sul livello dei servizi. Totale: 3,75 milioni di EUR. Tale importo ha costituito l'intero bilancio del CERT-UE, comprendendo la formazione, l'hardware, il software, le missioni, il supporto, gli agenti contrattuali e le conferenze.

Una volta entrato in vigore il regolamento, si prevede che le risorse future del CERT-UE saranno:

- posti permanenti 34 ETP;

- agenti contrattuali 15 ETP;

- totale: 49 ETP, con un aumento netto quindi di 11 ETP.

La variazione nel rapporto fra posti permanenti e agenti contrattuali è volta a rimediare alle difficoltà persistenti relative alle assunzioni e al mantenimento di professionisti della cibersicurezza di livello elevato, data la loro scarsità sul mercato del lavoro.

1 agente contrattuale ETP sarà inoltre necessario presso la Direzione generale dell'Informatica della Commissione per sostenere l'IICB (comitato interistituzionale per la cibersicurezza).

Saranno quindi necessari in tutto 21 ETP supplementari ai fini dell'attuazione del regolamento (20 ETP per il CERT-UE e 1 per la Direzione generale dell'Informatica della Commissione). Ciò sarà compensato da una riduzione parallela di 9 posti di agenti contrattuali ETP presso il CERT-UE, precedentemente finanziati da entrate con destinazione specifica nel quadro di accordi sul livello dei servizi.

Il bilancio per le risorse non umane del CERT-UE nel 2024, dopo il periodo di transizione, coprirà i compiti di cui sopra, alle lettere da a) a e), e dovrebbe essere finanziato come segue:

- 8,921 milioni di EUR all'anno provenienti dalle istituzioni dell'Unione, finanziati nell'ambito della rubrica 7 del bilancio dell'Unione;

- 2,459 milioni di EUR provenienti dalle istituzioni, organi e agenzie dell'Unione, finanziati nell'ambito delle rubriche da 1 a 6 del bilancio dell'Unione;

- 2,670 milioni di EUR provenienti dalle istituzioni, organi e agenzie dell'Unione autofinanziati.

- Bilancio totale del CERT-UE: 14,05 milioni di EUR.

I compiti di cui all'articolo 12, paragrafo 5, non sono descritti nel catalogo dei servizi, e sono addebitabili. Si tratta di servizi accessori, per lo più temporanei, che rappresentano degli importi relativamente bassi. I costi di tali servizi saranno recuperati dai loro beneficiari per mezzo di accordi sul livello dei servizi o accordi scritti.

Per quanto riguarda i contributi al personale del CERT-UE: le istituzioni e i principali organi dell'Unione contribuiranno con una quota equa che è proporzionale alla propria quota rispettiva di posti permanenti AD. Occorre verificare se la BCE e la BEI possono anch'esse apportare un contributo equo distaccando personale permanente.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La Commissione, coadiuvata dall'IICB e dal CERT-UE, riesaminerà periodicamente il funzionamento del regolamento e riferirà al Parlamento europeo e al Consiglio, la prima volta entro 48 mesi dalla sua entrata in vigore, e successivamente ogni tre anni.

Le fonti di dati utilizzate per i riesami dovrebbero provenire principalmente dall'IICB e dal CERT-UE. Ove necessario potrebbero inoltre essere usati specifici strumenti di raccolta di dati, ad es. inchieste presso le istituzioni, gli organi e le agenzie dell'Unione, l'ENISA o la rete di CSIRT.

2.2. Sistema di gestione e di controllo

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

Le azioni derivanti dal regolamento saranno gestite all'interno di ogni istituzione, organo e agenzia dell'Unione conformemente alle loro disposizioni legislative e regolamentari applicabili in materia.

La gestione amministrativa e finanziaria delle attività del CERT-UE è integrata nell'amministrazione della Commissione e ne segue i meccanismi di gestione e attuazione, le modalità di pagamento e i controlli applicabili.

Il revisore contabile interno della Commissione esercita nei confronti del CERT-UE le stesse competenze di cui dispone nei confronti dei servizi della Commissione

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

Rischio molto basso, dato che il CERT-UE è già collegato amministrativamente, come task force della Commissione, al direttore generale dell'informatica, e l'IICB segue il modello dell'attuale comitato direttivo del CERT-UE. L'ecosistema di gestione finanziaria e controllo interno è quindi già predisposto.

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

Esistono già procedure ben collaudate per gli appalti, la gestione finanziaria e il controllo. Il rapporto costo/efficacia dei controlli e i livelli di rischio di errore corrispondono a quelli in ogni istituzione, organo o agenzia dell'Unione, e a quelli della Commissione per le attività del CERT-UE.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Alle attività del CERT-UE si applicano i sistemi di gestione finanziaria e di controllo interno della Commissione.

Nella lotta contro la frode, la corruzione e altre attività illegali si applicano senza limitazioni le disposizioni del 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);

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

<u>Secondo l'ordine</u> delle rubriche del quadro finanziario pluriennale e delle linee di bilancio

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Contributo			
	Numero	Diss./Non diss.f[13].	di paesi EFTA[14]	di paesi candidati[15]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
Da 1 a 6	Linee di bilancio riguardanti i contributi dell'Unione agli organi e alle agenzie decentrate	Diss.	NO	NO	NO	NO
7.	Linee di bilancio riguardanti le retribuzioni del personale, la spesa informatica e altre spese amministrative nelle varie sezioni del bilancio dell'UE	Non diss.	NO	NO	NO	NO

- Nuove linee di bilancio di cui è chiesta la creazione

<u>Secondo l'ordine</u> delle rubriche del quadro finanziario pluriennale e delle linee di bilancio

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Contributo			
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	Nessuna.		SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

[13] Diss. = stanziamenti dissociati/Non diss. = stanziamenti non dissociati.
[14] EFTA: Associazione europea di libero scambio.
[15] 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:

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Da 1 a 6	Rubriche riguardanti i contributi agli organi e alle agenzie decentrate

DG: Varie			Anno **2023.**	Anno **2024.**	Anno **2025.**	Anno **2026.**	Anno **2027.**	**TOTALE**
○ Stanziamenti operativi								
Linee di bilancio riguardanti i contributi dell'Unione alle agenzie decentrate (xx 10 xx xx)[16]	Impegni	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Stanziamenti amministrativi finanziati dalla dotazione di programmi specifici[17]								
Linea di bilancio		(3)						
TOTALE stanziamenti per la DG: Varie	Impegni	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Secondo la nomenclatura di bilancio ufficiale.

[17] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

○ TOTALE stanziamenti operativi	Impegni	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici		(6)						
TOTALE stanziamenti a titolo delle RUBRICHE da 1 a 6 del quadro finanziario pluriennale	Impegni	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Se la proposta/iniziativa incide su più rubriche operative, ricopiare nella sezione sotto:

○ TOTALE stanziamenti operativi (tutte le rubriche operative)	Impegni	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici (tutte le rubriche operative)		(6)						
TOTALE stanziamenti a titolo delle RUBRICHE da 1 a 6 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamenti	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Rubrica del quadro finanziario pluriennale	**7**	"Spese amministrative"

Sezione da compilare utilizzando i "dati di bilancio di natura amministrativa" che saranno introdotti nell'allegato della scheda finanziaria legislativa (allegato V delle norme interne), caricata su DECIDE a fini di consultazioni interservizi.

Mio EUR (al terzo decimale)

		Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	**Anno 2027**	**TOTALE**
DG: DIGIT (CERT-EU)							
○ Risorse umane		1,184	2,126	2,754	3,225	3,225	12,514
○ Altre spese amministrative		7,938	8,921	8,921	8,921	8,921	43,622
TOTALE DG DIGIT (CERT-EU)	Stanziamenti	9,122	11,047	11,675	12,146	12,146	56,136

TOTALE stanziamenti a titolo della RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	9,122	11,047	11,675	12,146	12,146	**56,136**

Mio EUR (al terzo decimale)

		Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	**TOTALE**
TOTALE stanziamenti a titolo delle RUBRICHE da 1 a 7 del quadro finanziario pluriennale	Impegni	11,581	13,506	14,134	14,605	14,605	68,429
	Pagamenti	11,581	13,506	14,134	14,605	14,605	68,429

(*) I contributi delle istituzioni, organi e agenzie dell'Unione autofinanziati sono stimati a 2,670 milioni di EUR all'anno (totale per i cinque anni, 13,350 milioni di EUR) I contributi costituiranno entrate con destinazione specifica per il CERT-UE. Le tabelle di cui sopra comprendono solo l'incidenza totale stimata sul bilancio dell'Unione e non includono tali contributi.

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **N**		Anno **N+1**		Anno **N+2**		Anno **N+3**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**	
			RISULTATI															
	Tipo[18]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[19]…																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale dell'obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		
- Risultato																		
Totale parziale dell'obiettivo specifico 2																		
TOTALI																		

[18] I risultati sono i prodotti e i servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[19] Come descritto al punto 1.4.2. "Obiettivi specifici..."

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:

Mio EUR (al terzo decimale)

	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	**TOTALE**
RUBRICA 7 del quadro finanziario pluriennale						
Risorse umane						
Personale permanente (gradi AD)	1,099	2,041	2,669	3,14	3,14	12,089
Agenti contrattuali	0,085	0,085	0,085	0,085	0,085	0,425
Altre spese amministrative	7,938	8,921	8,921	8,921	8,921	43,622
Totale parziale della RUBRICA 7 del quadro finanziario pluriennale	9,122	11,047	11,675	12,146	12,146	56,136

Esclusa la RUBRICA 7[20] del quadro finanziario pluriennale						
Risorse umane						
Altre spese di natura amministrativa						
Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale						

TOTALE	9,122	11,047	11,675	12,146	12,146	56,136

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese amministrative è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, alla luce dei vincoli di bilancio.

[20] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☑ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

		Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027		
O Posti della tabella dell'organico (funzionari e agenti temporanei)								
20 01 02 01 (sede e uffici di rappresentanza della Commissione)		7	13	17	20	20		
20 01 02 03 (delegazioni)								
01 01 01 01 (ricerca indiretta)								
01 01 01 11 (ricerca diretta)								
Altre linee di bilancio (specificare)								
O Personale esterno (in equivalenti a tempo pieno: ETP)[21]								
20 02 01 (AC, END, INT dalla dotazione globale)		1	1	1	1	1		
20 02 03 (AC, AL, END, INT e JPD nelle delegazioni)								
XX 01 xx **yy zz** [22]	- in sede							
	- nelle delegazioni							
01 01 01 02 (AC, END, INT - ricerca indiretta)								
01 01 01 12 (AC, END, INT - ricerca diretta)								
Altre linee di bilancio (specificare)								
TOTALE		**8**	**14**	**18**	**21**	**21**		

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	I funzionari svolgeranno i compiti e le attività del CERT-UE conformemente al regolamento, in particolare ai capi IV e V.
Personale esterno	L'agente contrattuale coadiuverà nelle funzioni di segreteria del comitato interistituzionale per la cibersicurezza.

[21] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

[22] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

La proposta/iniziativa:

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

Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti. Allegare una tabella Excel in caso di riprogrammazione maggiore.

– ☐ comporta l'utilizzo del margine non assegnato della pertinente rubrica del QFP e/o l'utilizzo degli strumenti speciali quali definiti nel regolamento QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate, gli importi corrispondenti e gli strumenti proposti.

– ☐ comporta una revisione del QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– ☑ non prevede cofinanziamenti di terzi[23]

– ☐ prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**[24]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE stanziamenti cofinanziati								

[23] Le entrate con destinazione specifica derivanti dalla fornitura sporadica di servizi a organizzazioni non utenti di cui all'articolo 12, paragrafo 5, lettera c), non sono state stimate perché dovrebbero essere marginali.

[24] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021. e così per gli anni a seguire.

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:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[25]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo …….								

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

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

[25] 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.