Consiglio dell'Unione europea

Bruxelles, 31 ottobre 2022
(OR. en)

14128/22

Fascicolo interistituzionale: 2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTA PUNTO "I/A"

Origine:	Segretariato generale del Consiglio
Destinatario:	Comitato dei rappresentanti permanenti (parte seconda)/Consiglio
n. doc. prec.:	10097/5/22 REV 5
n. doc. Comm.:	7474/22 + ADD 1
Oggetto:	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 - Orientamento generale

INTRODUZIONE

1. Il 22 marzo 2022 la Commissione ha adottato la 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. La proposta era una delle misure previste nella strategia dell'UE in materia di cibersicurezza per il decennio digitale[1] che mira a rafforzare la resilienza collettiva dell'Unione contro le minacce informatiche.

[1] Doc. 14133/20.

Nelle sue conclusioni del 22 marzo 2021 su tale strategia[2], il Consiglio ha sottolineato che la cibersicurezza è "fondamental[e] per il funzionamento della pubblica amministrazione e delle istituzioni a livello sia nazionale che dell'UE, nonché per la nostra società e per l'economia nel suo complesso".

2. La proposta della Commissione, basata sull'articolo 298 del trattato sul funzionamento dell'Unione europea, mira ad aumentare il livello di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione istituendo un quadro comune, nel rispetto dell'autonomia di ciascun soggetto dell'Unione. In particolare, gli obiettivi della proposta sono:

   – consolidare il mandato e il finanziamento del CERT-UE (squadra interistituzionale autonoma di pronto intervento informatico dei soggetti dell'Unione);

   – istituire una struttura interistituzionale (comitato interistituzionale per la cibersicurezza – IICB) che riunisca i rappresentanti di tutti i soggetti dell'Unione al fine di garantire la corretta attuazione del regolamento;

   – introdurre l'obbligo per i soggetti dell'Unione di condividere informazioni (non classificate) sugli incidenti con il CERT-UE e di notificare minacce, vulnerabilità e incidenti significativi; e

   – promuovere il coordinamento e la cooperazione nel quadro della risposta a incidenti significativi.

3. Il Parlamento europeo ha nominato Henna Virkkunen (PPE) relatrice della commissione ITRE, competente per il merito. Il progetto di relazione è stato pubblicato il 7 ottobre 2022.

4. Il Garante europeo della protezione dei dati ha formulato il suo parere il 17 maggio 2022[3].

[2] Doc. 6722/21.
[3] Doc. 9252/22.

5. Al Consiglio, l'esame della proposta in sede di gruppo orizzontale "Questioni riguardanti il ciberspazio" è iniziato durante la presidenza francese, il 29 marzo 2022. La presidenza francese ha preparato il primo testo di compromesso, discusso in sede di gruppo orizzontale "Questioni riguardanti il ciberspazio" nel giugno 2022, e ha presentato al Consiglio una relazione sullo stato di avanzamento dei lavori[4] il 21 giugno 2022.

6. Nel corso della presidenza ceca, il gruppo orizzontale "Questioni riguardanti il ciberspazio" ha dedicato otto riunioni[5] alle discussioni sulla proposta e su diversi testi di compromesso che si sono susseguiti.

7. Il 23 maggio 2022 la presidenza ha chiesto un parere al comitato per la sicurezza del Consiglio sugli aspetti della proposta connessi alla sicurezza delle informazioni, e in particolare alle informazioni classificate. Il comitato per la sicurezza del Consiglio ha reso il suo parere il 19 settembre 2022[6]. Come suggerito dal comitato per la sicurezza del Consiglio, le informazioni classificate UE sono state esplicitamente escluse dall'ambito di applicazione del regolamento. Le disposizioni relative alle esenzioni dagli obblighi di condivisione e segnalazione per quanto riguarda le informazioni ricevute dall'esterno dei soggetti dell'Unione sono state modificate di conseguenza.

8. Il 28 ottobre 2022 il gruppo orizzontale "Questioni riguardanti il ciberspazio" ha raggiunto un accordo sul compromesso della presidenza riportato nell'allegato.

---

4 Doc. 9719/22.
5 il 6 e 20 luglio, il 13, 21 e 28 settembre e il 5, 19 e 28 ottobre 2022.
6 Doc. 12603/22 + COR 1.

QUESTIONI PRINCIPALI

9. Gli Stati membri hanno accolto con favore la proposta, in quanto tempestiva e complementare alla futura direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva "NIS 2"), e ne hanno sostenuto gli obiettivi generali. Tuttavia, hanno chiesto ulteriori allineamenti alla direttiva "NIS 2" e una maggiore reciprocità nello scambio di informazioni tra i soggetti dell'Unione e gli Stati membri e hanno evidenziato il carattere eccessivamente volontario di alcune delle misure proposte. Gli Stati membri hanno anche espresso la loro preferenza per la soppressione dei riferimenti all'unità congiunta per il ciberspazio, il cui mandato e la cui composizione non sono ancora definiti.

10. Sulla base delle discussioni a livello del gruppo orizzontale "Questioni riguardanti il ciberspazio", le principali questioni politiche individuate riguardano i seguenti punti.

a) Allineamento alla futura direttiva "NIS 2"

Come richiesto dagli Stati membri, sono stati apportati ulteriori allineamenti alla futura direttiva "NIS 2", tra cui i seguenti:

- numerose definizioni (articolo 3) sono state allineate a quelle della "NIS 2";
- è stato inserito un nuovo articolo 7 bis sulle valutazioni inter pares volontarie, in linea con la "NIS 2", adeguate alle esigenze dei soggetti dell'Unione;
- gli obblighi di segnalazione di cui all'articolo 20 sono stati allineati a quelli della "NIS 2".

b) Composizione del comitato interistituzionale per la cibersicurezza (IICB) (articolo 9)

A seguito delle discussioni sull'adeguato coinvolgimento dei rappresentanti degli Stati membri nei lavori dell'IICB, è stato raggiunto un compromesso mediante una dichiarazione del Consiglio da iscrivere nel processo verbale.

c) Autonomia istituzionale

Si è arrivati a un approccio equilibrato tra la volontà degli Stati membri di rafforzare i meccanismi di conformità e la necessità di rispettare il principio dell'autonomia istituzionale, in particolare per quanto riguarda gli audit e le misure disciplinari (articolo 11).

Infine, è stato eliminato dal considerando 8 il riferimento a una specifica percentuale del bilancio informatico dedicata alla cibersicurezza.

CONCLUSIONE

11. Si invita il Comitato dei rappresentanti permanenti a:

a) approvare il testo di compromesso che figura nell'allegato, che costituirà quindi il mandato per i negoziati con il Parlamento europeo;

b) invitare il Consiglio ad approvare nella sessione del 18 novembre 2022 il testo di compromesso che figura nell'allegato e a iscrivere nel processo verbale la dichiarazione del Consiglio che figura nell'addendum al presente documento.

ALLEGATO

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 su**i soggetti** [...] 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 de**i soggetti** [...] 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 **soggetto** [...] 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 de**i soggetti** [...] 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. **In aggiunta, i soggetti dell'Unione gestiscono grandi quantità di informazioni spesso sensibili provenienti dagli Stati membri; gli incidenti potrebbero quindi incidere negativamente anche su questi ultimi. Per questo motivo, la cibersicurezza dei soggetti dell'Unione è di grande importanza anche per gli Stati membri. Le informazioni specifiche su un incidente possono inoltre facilitare il rilevamento di minacce informatiche o incidenti analoghi che interessano gli Stati membri.**

(4) **I soggetti** [...] 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 **i soggetti** [...] dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso **l'attuazione di misure di 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 [...] **i soggetti** 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 [...] **soggetto** dell'Unione stabilisca 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 [...]. **Il quadro dovrebbe stabilire politiche in materia di cibersicurezza, comprese procedure per valutare l'efficacia delle misure di cibersicurezza attuate. Il quadro dovrebbe basarsi su un approccio multirischio che miri a proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti dell'Unione e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi, trattati o accessibili tramite i sistemi informatici e di rete. Il quadro dovrebbe rispecchiare i risultati dell'analisi dei rischi, tenendo conto di tutti i pertinenti rischi tecnici, operativi e organizzativi per la cibersicurezza del soggetto dell'Unione interessato.**

(6 bis) Per gestire i rischi individuati nell'ambito del quadro, ciascun soggetto dell'Unione dovrebbe garantire l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate. Tali misure dovrebbero riguardare i settori, comprese le misure di cibersicurezza di cui al presente regolamento intese a rafforzare la cibersicurezza di ciascun soggetto dell'Unione.

(6 ter) Le risorse e i rischi individuati nel quadro nonché le conclusioni tratte dalle valutazioni di maturità periodiche dovrebbero essere rispecchiate nel piano di cibersicurezza stabilito da ciascun soggetto dell'Unione. Il piano di cibersicurezza dovrebbe includere le misure di cibersicurezza adottate, con l'obiettivo di aumentare la cibersicurezza complessiva del soggetto dell'Unione interessato.

(6 quater) Poiché garantire la cibersicurezza è un processo continuo, l'adeguatezza e l'efficacia di tutte le misure dovrebbero essere riviste periodicamente alla luce dell'evoluzione dei rischi, delle risorse e della maturità dei soggetti dell'Unione. Il quadro dovrebbe essere riesaminato periodicamente e almeno ogni tre anni, mentre il piano di cibersicurezza dovrebbe essere rivisto almeno ogni due anni oppure a seguito di ciascuna valutazione di maturità o di ciascun riesame del quadro.

(6 quinquies) I soggetti dell'Unione dovrebbero scambiarsi periodicamente informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche pertinenti, garantendo nel contempo la riservatezza e la tutela adeguata delle informazioni fornite dal soggetto dell'Unione segnalante.

(6 sexies) È opportuno attuare un meccanismo per garantire l'efficacia dello scambio di informazioni, del coordinamento e della cooperazione dei soggetti dell'Unione in caso di incidenti gravi, compresa una chiara individuazione dei ruoli e delle responsabilità dei soggetti dell'Unione coinvolti. Le informazioni scambiate dovrebbero essere tenute in considerazione dal punto di contatto designato per la rete EU-CyCLONe al momento di condividere le informazioni pertinenti con quest'ultima quale contributo alla conoscenza situazionale condivisa.

(7) Le differenze esistenti fra [...] **i soggetti** 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 [...] **dei soggetti** dell'Unione o che ne intacchi l'autonomia istituzionale. Tali [...] **soggetti dell'Unione** dovrebbero quindi istituire i propri quadri di gestione, di governance e di controllo dei rischi per la cibersicurezza **nonché i propri piani di cibersicurezza**, e dovrebbero adottare [...] **misure** [...] di cibersicurezza. **Nell'attuare tali misure si dovrebbe tenere debitamente conto delle sinergie esistenti tra i soggetti dell'Unione, ai fini di una corretta gestione delle risorse e dell'ottimizzazione dei costi. È inoltre opportuno tenere debitamente conto del fatto che le misure non incidono negativamente sull'efficienza dello scambio di informazioni e delle operazioni dei soggetti dell'Unione con altri soggetti dell'Unione e con le autorità nazionali competenti.**

(8) Per evitare di imporre un onere finanziario e amministrativo sproporzionato [...] **ai soggetti** 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 [...] **soggetto** dell'Unione dovrebbe mirare a stanziare un'adeguata percentuale del suo bilancio informatico per migliorare il livello di cibersicurezza [...]. **La valutazione di maturità dovrebbe inoltre determinare se la spesa per la cibersicurezza del soggetto dell'Unione è proporzionata ai rischi cui è esposto quest'ultimo.**

(9) Un livello comune elevato di cibersicurezza richiede che tale aspetto sia soggetto alla sorveglianza del livello di dirigenza più elevato di ogni [...] **soggetto** dell'Unione. [...] **Il livello di dirigenza più elevato dovrebbe sorvegliare l'attuazione del presente regolamento, inclusa l'istituzione del quadro di gestione, di governance e di controllo dei rischi e dei piani di cibersicurezza, ivi comprese misure di cibersicurezza**. Occuparsi della cultura della cibersicurezza, ossia della pratica quotidiana della cibersicurezza, è parte integrante di [...] **un quadro** di cibersicurezza [...] in tutti i **soggetti** dell'Unione.

(10) [...] [...] Le misure **di cibersicurezza** dovrebbero far parte [...] **del piano di** 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 **lo stato dell'arte e, se del caso, le pertinenti norme europee e internazionali nonché** 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. **Se del caso, il CERT-UE dovrebbe cooperare con l'ENISA.**

(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[7]. [...] **Il presente regolamento** dovrebbe [...] **fornire una serie completa di norme sull'organizzazione, il funzionamento e l'operatività del CERT-UE. Le disposizioni del presente regolamento prevalgono sulle disposizioni dell'accordo interistituzionale sull'organizzazione e il funzionamento del CERT-UE concluso nel dicembre 2017**.

[...]

GU C 12 del 13.1.2018, pag. 1.

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

(13 bis) Il presente regolamento stabilisce un approccio in più fasi alla segnalazione degli incidenti significativi al fine di trovare il giusto equilibrio tra, da un lato, una segnalazione rapida che contribuisca ad attenuare la potenziale diffusione di incidenti significativi e consenta ai soggetti dell'Unione di chiedere assistenza e, dall'altro, una segnalazione approfondita che tragga insegnamenti preziosi dai singoli incidenti e migliori nel tempo la ciberresilienza dei singoli soggetti dell'Unione. A tale proposito, il presente regolamento dovrebbe includere la segnalazione di incidenti che, sulla base di una valutazione iniziale condotta dal soggetto dell'Unione, potrebbero causare gravi perturbazioni operative per il funzionamento del soggetto dell'Unione o perdite finanziarie per il soggetto dell'Unione interessato, o interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali. Detta valutazione iniziale dovrebbe tenere conto, tra l'altro, dei sistemi informatici e di rete interessati, in particolare della loro importanza per il funzionamento del soggetto dell'Unione, della gravità e delle caratteristiche tecniche di una minaccia informatica e delle eventuali vulnerabilità sottostanti che vengono sfruttate, nonché dell'esperienza del soggetto dell'Unione in caso di incidenti simili. Indicatori quali la misura in cui il funzionamento del soggetto dell'Unione è interessato, la durata di un incidente o il numero di persone fisiche o giuridiche interessate potrebbero svolgere un ruolo importante nel determinare se la perturbazione operativa sia grave o meno.

(13 ter) Poiché l'infrastruttura e le reti del pertinente soggetto dell'Unione e dello Stato membro in cui è situato tale soggetto dell'Unione sono interconnesse, è fondamentale che detto Stato membro sia informato senza indebito ritardo di un incidente significativo all'interno di tale soggetto dell'Unione. A tal fine, il soggetto dell'Unione interessato dovrebbe informare l'omologo nazionale del CERT-UE, designato dallo Stato membro conformemente alla direttiva [proposta NIS 2], rispettando gli stessi termini entro cui dovrebbe segnalare un incidente significativo al CERT-UE. Quest'ultimo, a sua volta, dovrebbe informare tale omologo nazionale quando viene a conoscenza di un incidente significativo all'interno dello Stato membro, a meno che non sia già stato segnalato dal soggetto dell'Unione interessato.

(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, **al fine di contribuire all'instaurarsi di un livello comune elevato di cibersicurezza nei soggetti dell'Unione**, dovrebbe **svolgere un ruolo esclusivo** [...] [...] **nel monitoraggio** dell'attuazione del presente regolamento da parte [...] **dei soggetti** dell'Unione e [...] **nella supervisione** dell'attuazione delle priorità e degli obiettivi generali da parte del CERT-UE **nonché nella fornitura** a tale centro **di** una direzione strategica. L'IICB dovrebbe **pertanto** garantire la rappresentanza delle istituzioni e includere rappresentanti delle agenzie e degli organi attraverso la rete delle agenzie dell'Unione. **L'organizzazione e il funzionamento dell'IICB dovrebbero essere ulteriormente disciplinati dal suo regolamento interno, che può comprendere un'ulteriore precisazione delle riunioni periodiche dell'IICB, compresi raduni annuali a livello politico in cui i rappresentanti del livello di dirigenza più elevato di ciascun membro dell'IICB consentirebbero all'IICB di tenere discussioni strategiche e gli fornirebbero orientamenti strategici. Inoltre, l'IICB può istituire un comitato esecutivo incaricato di assisterlo nei suoi lavori e di delegargli alcuni dei suoi compiti e poteri, in particolare in termini di compiti che richiedono [...] competenze specifiche dei suoi membri, ad esempio l'approvazione del catalogo dei servizi e dei successivi aggiornamenti, le modalità degli accordi sul livello dei servizi, le valutazioni dei documenti e delle relazioni presentati dai soggetti dell'Unione all'IICB a norma del presente regolamento o i compiti relativi alla preparazione delle decisioni sulle misure di conformità emanate dall'IICB e al monitoraggio della loro attuazione**. **L'IICB dovrebbe stabilire il regolamento interno del comitato esecutivo, compresi i suoi compiti e i suoi poteri.**

(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 [...] **i soggetti** dell'Unione sono esortati ad adottare entro un termine stabilito. **L'IICB può chiedere al CERT-UE di emanare, ritirare o modificare una proposta relativa a documenti di orientamento o a una raccomandazione, o un invito a intervenire.**

(16) L'IICB dovrebbe controllare l'osservanza del presente regolamento come pure il seguito dato ai documenti di orientamento e alle raccomandazioni nonché agli inviti a intervenire [...]. 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 [...] **i soggetti** dell'Unione e altri portatori di interessi a seconda delle necessità. [...] **Qualora constati che i soggetti dell'Unione non hanno applicato o attuato il presente regolamento, compresi i documenti di orientamento, le raccomandazioni o gli inviti a intervenire emanati ai sensi del presente regolamento, l'IICB può, ferme restando le procedure interne del pertinente soggetto dell'Unione, procedere con le misure di conformità. Il sistema di misure di conformità dovrebbe essere utilizzato ricorrendo a una severità progressiva, il che significa che, nell'adottare le misure di conformità, l'IICB dovrebbe iniziare con un avvertimento quale misura meno severa e, se necessario, inasprire le misure fino a quella più severa, consistente nell'emissione di un avviso che raccomandi la sospensione temporanea dei flussi di dati verso il soggetto dell'Unione interessato, che sarebbe applicata in casi eccezionali di inosservanza a lungo termine, deliberata e/o grave, da parte del soggetto interessato, degli obblighi ad esso incombenti a norma del presente regolamento.**

(16 bis) L'avvertimento rappresenta la misura di conformità meno severa, intesa a ovviare alle carenze individuate del soggetto dell'Unione e comprendente raccomandazioni relative alla modifica dei suoi documenti sulla cibersicurezza entro un periodo di tempo specificato. L'avvertimento dovrebbe essere disponibile per tutti i soggetti dell'Unione, salvo eventuali opportune restrizioni a norma del presente regolamento.

(16 ter) L'IICB può inoltre raccomandare lo svolgimento di un audit di un soggetto dell'Unione. A tal fine, il soggetto dell'Unione può utilizzare la propria funzione di audit interno. L'IICB potrebbe inoltre richiedere lo svolgimento di un audit a cura di un servizio di audit di terzi, compreso un prestatore di servizi del settore privato concordato di comune accordo.

(16 quater) Sulla base dei risultati di un audit svolto su raccomandazione o su richiesta dell'IICB, quest'ultimo può inoltre chiedere al soggetto dell'Unione di rendere conformi alle disposizioni del presente regolamento la gestione, la governance e il controllo dei rischi per la cibersicurezza.

(16 quinquies) Poiché gli Stati membri condividono con i pertinenti soggetti dell'Unione informazioni che possono essere di natura sensibile, la cibersicurezza del destinatario di tali informazioni è fondamentale per gli Stati membri. Pertanto, in casi eccezionali di inosservanza a lungo termine, deliberata, ripetuta e/o grave dell'obbligo incombente al soggetto dell'Unione, l'IICB può emanare, come misura di ultima istanza, un avviso rivolto a tutti gli Stati membri e soggetti dell'Unione che raccomandi la sospensione temporanea dei flussi di dati verso il soggetto dell'Unione, che dovrebbe essere mantenuta fino ad avvenuta correzione dello stato della cibersicurezza di tale soggetto. Detto avviso dovrebbe essere comunicato a tutti gli Stati membri e soggetti dell'Unione mediante adeguati canali di comunicazione sicuri.

(16 sexies) Al fine di garantire la corretta attuazione del presente regolamento, qualora ritenga che una violazione persistente del presente regolamento da parte di un soggetto dell'Unione sia stata causata direttamente dalle azioni o dall'omissione di un membro del suo personale, anche al livello di dirigenza più elevato, l'IICB dovrebbe chiedere al soggetto dell'Unione interessato di adottare misure adeguate nei confronti di tale membro del personale, in conformità dello statuto dei funzionari e di altre norme equivalenti applicabili in determinati soggetti dell'Unione. Tali azioni possono comprendere, ad esempio, procedimenti disciplinari e, ove opportuno, nel caso specifico delle agenzie dell'Unione, una richiesta all'autorità competente di adottare le misure necessarie in relazione all'eventuale rimozione dall'incarico della persona che potrebbe essere responsabile della violazione persistente del presente regolamento.

(17) Il CERT-UE dovrebbe avere la missione di contribuire alla sicurezza dell'ambiente informatico di [...] **tutti i soggetti** dell'Unione. **Nel valutare se fornire consulenza o contributi tecnici su importanti questioni strategiche su richiesta di un soggetto dell'Unione, il CERT-UE dovrebbe garantire che ciò non ostacoli l'adempimento degli altri compiti di cui al presente regolamento.**

(17 bis) Il CERT-UE dovrebbe fungere da equivalente del coordinatore designato per [...] **i soggetti** dell'Unione, ai fini della divulgazione coordinata delle vulnerabilità al registro europeo delle vulnerabilità di cui all'articolo 6 della direttiva [proposta NIS 2] **e dovrebbe sviluppare una politica sulla gestione delle vulnerabilità, che comprenda la promozione e l'agevolazione della divulgazione coordinata volontaria delle vulnerabilità.**

[...]

(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[8] 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.

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

(20) Nel sostenere la cibersicurezza operativa, il CERT-UE dovrebbe avvalersi delle competenze disponibili dell'Agenzia dell'Unione europea per la cibersicurezza **(ENISA)** attraverso una cooperazione strutturata di cui al regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[9]. 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'[...]**ENISA** per quanto riguarda l'analisi delle minacce e dovrebbe condividere periodicamente con l'Agenzia la sua relazione sul panorama delle minacce.

[...]

(22) **Le attività e il trattamento delle informazioni del CERT-UE a norma del presente regolamento possono comportare il trattamento di dati personali.** 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[11]. **Se, a norma del presente regolamento, i dati personali sono trasmessi a destinatari stabiliti nell'Unione diversi dai soggetti dell'Unione, ciò dovrebbe avvenire in conformità dell'articolo 9 del regolamento (UE) 2018/1725.**

---

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

11 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).

(23) Il trattamento delle informazioni da parte del CERT-UE e [...] **dei soggetti** dell'Unione dovrebbe essere in linea con le norme **applicabili** [...] sulla sicurezza delle informazioni[...]. [...]

(23 bis) Ai fini della condivisione delle informazioni, sono utilizzati contrassegni visibili per indicare che i destinatari delle informazioni devono applicare limiti di condivisione sulla base, in particolare, di accordi di non divulgazione o di accordi di non divulgazione informali quali il protocollo TLP (*Traffic Light Protocol*) o altre indicazioni chiare da parte della fonte. Il protocollo TLP deve essere inteso come uno strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e in alcuni centri di analisi e condivisione delle informazioni.

(24) **Il presente regolamento e i nuovi compiti assegnati al CERT-UE non avranno alcun effetto sulle spese totali nell'ambito del quadro finanziario pluriennale.** Poiché i servizi e i compiti del CERT-UE sono svolti nell'interesse di [...] **tutti i soggetti** dell'Unione, ogni [...] **soggetto** 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 [...] **dei soggetti** dell'Unione. **Tutti i soggetti dell'Unione e le rispettive amministrazioni dovrebbero garantire l'ottimizzazione delle loro risorse al livello attuale e rafforzare gli incrementi di efficienza, anche approfondendo la cooperazione interistituzionale nel settore della cibersicurezza. Si dovrebbe pertanto privilegiare un approccio congiunto alla messa in comune delle spese amministrative rispetto alla spesa individuale dei soggetti dell'Unione.**

(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. **Inoltre, la Corte dei conti europea è invitata a valutare periodicamente il funzionamento del CERT-UE,**

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto

1. Il presente regolamento stabilisce **misure volte a conseguire un livello comune elevato di cibersicurezza nei soggetti dell'Unione** [...]

2. A tal fine, il presente regolamento stabilisce:

c) l'obbligo, per [...] **ciascun soggetto** dell'Unione, di stabilire un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza;

d) l'obbligo, per [...] **i soggetti** dell'Unione di gestione e di segnalazione dei rischi per la cibersicurezza **e di condivisione delle informazioni**;

e) norme riguardanti l'organizzazione**,** [...] il funzionamento **e la gestione** [...] **della squadra interistituzionale autonoma di pronto intervento informatico** [...] **dei soggetti** dell'Unione (CERT-EU) nonché l'organizzazione**,** [...] il funzionamento **e la gestione** del comitato interistituzionale per la cibersicurezza **(IICB)**;

f) norme relative al monitoraggio dell'attuazione del presente regolamento.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica a [...] [...] **tutti i soggetti** dell'Unione nonché [...] al [...] CERT-EU e **all'IICB** [...].

2. Il presente regolamento si applica fatta salva l'autonomia istituzionale prevista dai trattati.

3. Ad eccezione dell'articolo 12, paragrafo 7, il presente regolamento non si applica ai sistemi informatici e di rete che trattano informazioni classificate UE (ICUE).

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) "[...] **soggetti** dell'Unione": le istituzioni, gli organi **e gli organismi** 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": [...] **un** sistema informatico e di rete [...] **quale definito all**'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 [...] **quale definita all**'articolo 4, punto 2, della direttiva [proposta NIS 2];

4) "cibersicurezza": la cibersicurezza [...] **quale definita all'articolo 2, punto 1, del regolamento (UE) 2019/881**;

5) "livello di dirigenza più elevato": un dirigente, un organo di gestione o di coordinamento e sorveglianza al livello amministrativo più alto, **con capacità di decisione**, tenuto conto dei sistemi di governance ad alto livello di ogni [...] **soggetto** dell'Unione;

(5 bis) "quasi incidente": un quasi incidente quale definito all'articolo 4, punto 4 bis, della direttiva [proposta NIS 2];

6) "incidente": un incidente [...] **quale definito all'**articolo 4, punto 5, della direttiva [proposta NIS 2];

[...]

8) "**incidente** grave [...]": qualsiasi incidente **che causa un livello di perturbazione superiore alla capacità di un soggetto dell'Unione e del CERT-UE di rispondervi o che ha un impatto significativo su almeno due soggetti dell'Unione;** [...]

9) "gestione degli incidenti": gestione degli incidenti [...] **quale definita all'**articolo 4, punto 6, della direttiva [proposta NIS 2];

10) "minaccia informatica": una minaccia informatica [...] **quale definita all**'articolo 2, punto 8, del regolamento (UE) 2019/881;

[...]

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

[...]

14) "rischio [...]": **un rischio ai sensi dell'articolo 4, punto 7 ter, della direttiva [proposta NIS 2]** [...];

[...]

[...]

Articolo 3 bis

Trattamento dei dati personali

1) Il trattamento dei dati personali a norma del presente regolamento da parte del CERT-UE, dell'IICB o dei soggetti dell'Unione è effettuato in conformità del regolamento (UE) 2018/1725.

2) Il CERT-UE, l'IICB e i soggetti dell'Unione trattano e scambiano dati personali nella misura necessaria e al solo scopo di adempiere i rispettivi obblighi previsti dal presente regolamento.

Capo II
MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA

Articolo 4

Quadro di gestione, di governance e di controllo dei rischi

1. Ogni [...] **soggetto** dell'Unione stabilisce il proprio quadro [...] di gestione, di governance e di controllo dei rischi per la cibersicurezza (il "quadro") a sostegno della propria missione [...]**.** [...] **Il quadro è soggetto** 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 non riservato [...] **del soggetto dell'Unione** interessat[...]**o**, compresi ogni ambiente informatico in loco, **la rete di tecnologie operativa,** 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 **è basato su un approccio multirischio e su una valutazione di maturità in conformità dell'articolo 6 con riguardo a tutti i pertinenti rischi tecnici, operativi e organizzativi che potrebbero incidere sulla cibersicurezza del soggetto dell'Unione interessato** [...].

2 bis. Il quadro definisce le politiche in materia di cibersicurezza, compresi gli obiettivi e le priorità per la sicurezza dei sistemi informatici e di rete, nonché le politiche e le procedure per valutare l'efficacia delle misure di gestione dei rischi per la cibersicurezza attuate e definire i ruoli e le responsabilità dei membri del personale.

2 ter. Il quadro è riesaminato periodicamente e almeno ogni tre anni, alla luce dell'evoluzione dei rischi, delle risorse e della maturità del soggetto dell'Unione.

3. Il livello di dirigenza più elevato di ogni [...] **soggetto** dell'Unione **sorveglia** [...] 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.

3 bis. Se del caso e fatta salva la sua responsabilità per l'attuazione del presente regolamento, il livello di dirigenza più elevato di ciascun soggetto dell'Unione può delegare ad altri alti funzionari all'interno del soggetto interessato obblighi specifici ai sensi del presente regolamento. Indipendentemente dall'eventuale delega dei suoi obblighi specifici, il livello di dirigenza più elevato può essere ritenuto responsabile del mancato rispetto, da parte dei soggetti, degli obblighi previsti dal presente regolamento.

3 ter. Il livello di dirigenza più elevato di ciascun soggetto dell'Unione garantisce che i soggetti dell'Unione approvino il piano di cibersicurezza che include misure di gestione dei rischi per la cibersicurezza, conformemente alla loro analisi dei rischi, in modo che il quadro sia attuato in conformità del presente regolamento.

[...]

5. Ogni [...] **soggetto** 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.

Il responsabile locale per la cibersicurezza agevola l'attuazione del presente regolamento e riferisce direttamente al livello di dirigenza più elevato periodicamente in merito allo stato di attuazione.

Fatto salvo il fatto che il responsabile locale per la cibersicurezza è un punto di contatto unico in ciascun soggetto dell'Unione, un soggetto dell'Unione può delegare determinati compiti di responsabile locale per la cibersicurezza in relazione all'attuazione del presente regolamento al CERT-UE sulla base di un accordo sul livello dei servizi concluso tra tale soggetto dell'Unione e il CERT-UE. L'IICB decide se la fornitura di tale servizio fa parte dei servizi di base del CERT-UE, tenendo conto delle risorse umane e finanziarie del soggetto dell'Unione interessato. Ciascun soggetto dell'Unione notifica senza indebito ritardo al CERT-UE i responsabili locali per la cibersicurezza nominati e le eventuali modifiche successive. Il CERT-UE tiene un elenco aggiornato periodicamente dei responsabili locali per la cibersicurezza nominati.

6. Gli alti funzionari ai sensi dell'articolo 29 , paragrafo 2, dello Statuto[12] o gli altri funzionari di livello equivalente di ciascun soggetto 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, nonché il loro impatto sulle attività dell'organizzazione.

12 Regolamento n. 259/68 del Consiglio, del 29 febbraio 1968, che definisce lo statuto dei funzionari delle Comunità europee nonché il regime applicabile agli altri agenti di tali Comunità (GU L 56 del 4 marzo 1968).

7. Ogni soggetto dell'Unione dispone di meccanismi efficaci per garantire che un'adeguata percentuale del suo bilancio informatico sia spesa per la cibersicurezza. Nella definizione di tale percentuale si tiene debitamente conto del quadro di riferimento.

Articolo 5

Misure di gestione dei rischi per la cibersicurezza [...]

1. [...] **Ciascun soggetto dell'Unione, sotto la sorveglianza del** livello di dirigenza più elevato [...] [...]**, garantisce l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi individuati nell'ambito del quadro di cui all'articolo 4, paragrafo 1, e per prevenire e/o ridurre al minimo l'impatto degli incidenti. Tenuto conto dello stato dell'arte e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, tali misure garantiscono un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi posti. Nel valutare la proporzionalità di tali misure si tiene debitamente conto del grado di esposizione del soggetto ai rischi, delle sue dimensioni, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico.**

[...]

3. Nell'attuazione delle misure di gestione dei rischi per la cibersicurezza nell'ambito dei loro piani di cibersicurezza, i soggetti dell'Unione considerano almeno i seguenti settori specifici, in linea con i documenti di orientamento e le raccomandazioni dell'IICB:

a) la politica in materia di cibersicurezza, in termini di specificazione degli strumenti e delle misure necessari per conseguire gli obiettivi e le priorità di cui all'articolo 4 e all'articolo 5, paragrafo 4;

b) l'analisi dei rischi e le politiche di sicurezza dei sistemi informatici;

c) l'organizzazione della cibersicurezza, compresa la definizione di ruoli e responsabilità;

d) la gestione delle risorse, compresi l'inventario delle risorse informatiche e la cartografia della rete informatica;

e) la sicurezza delle risorse umane e il controllo dell'accesso;

f) la sicurezza delle operazioni;

g) la sicurezza delle comunicazioni;

h) l'acquisizione, lo sviluppo e la manutenzione dei sistemi, comprese la gestione e la divulgazione delle vulnerabilità;

i) la sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti le relazioni tra ciascun soggetto dell'Unione e i suoi fornitori diretti o prestatori di servizi. I soggetti dell'Unione tengono conto delle vulnerabilità specifiche di ciascun fornitore diretto e prestatore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei loro fornitori e prestatori di servizi, comprese le loro procedure di sviluppo sicuro;

j) la gestione degli incidenti e la cooperazione con il CERT-UE, ad esempio mantenendo il monitoraggio della sicurezza e le pratiche di registrazione;

k) la gestione della continuità operativa, come la gestione di back up e il ripristino in caso di disastro, e la gestione delle crisi e

l) la promozione e lo sviluppo di programmi di educazione, competenze, sensibilizzazione, esercizio e formazione in materia di cibersicurezza.

4. Nell'attuazione delle misure di gestione dei rischi di cibersicurezza nell'ambito dei loro piani di cibersicurezza, i soggetti dell'Unione considerano almeno le seguenti specifiche misure di gestione dei rischi di cibersicurezza, in linea con i documenti di orientamento e le raccomandazioni dell'IICB:

a) gli obiettivi e le priorità per quanto riguarda l'uso di servizi di cloud computing ai sensi dell'articolo 4, punto 19, della direttiva [proposta NIS 2] e le modalità tecniche per consentire il telelavoro;

b) misure concrete per un uso futuro di principi zero trust, compreso un modello di sicurezza, e una strategia coordinata di cibersicurezza e di gestione dei sistemi basata sul riconoscimento dell'esistenza di minacce sia all'interno che all'esterno dei confini di rete tradizionali;

c) l'adozione dell'autenticazione a più fattori come norma in tutti i sistemi informatici e di rete;

d) l'introduzione di una catena di approvvigionamento del software sicura, attraverso criteri di sviluppo e valutazione sicuri del software;

e) il rafforzamento delle norme relative agli appalti, per facilitare il conseguimento di un livello comune elevato di cibersicurezza attraverso:

i) l'eliminazione degli ostacoli contrattuali che limitano la condivisione delle informazioni sugli incidenti, le vulnerabilità e le minacce informatiche fra i prestatori di servizi informatici e il CERT-UE, e

ii) l'obbligo contrattuale di segnalare gli incidenti, le vulnerabilità e le minacce informatiche, così come di avere predisposte adeguate misure di monitoraggio e risposta in caso di incidenti;

f) l'uso della crittografia e della cifratura, in particolare la cifratura da punto a punto;

g) i sistemi di comunicazione sicuri all'interno dell'organizzazione.

Articolo 6

Valutazioni di maturità

1. Ogni **soggetto** [...] dell'Unione svolge, **se del caso con l'assistenza di terzi specializzati**, almeno ogni tre anni **una** valutazione di maturità [...], che comprende tutti gli elementi del proprio ambiente TIC come descritto all'articolo 4, tenendo conto dei documenti di orientamento e delle raccomandazioni pertinenti adottati conformemente all'articolo 13.

2. L'IICB, su raccomandazione del CERT-UE e previa consultazione dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), adotta, entro quattro mesi dall'entrata in vigore del presente regolamento, orientamenti metodologici per lo svolgimento delle valutazioni di maturità.

3. Il soggetto dell'Unione sottopone la valutazione di maturità [...], una volta ultimata, all'IICB. La prima valutazione di maturità si svolge al più tardi [12 mesi dopo l'entrata in vigore del presente regolamento].

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 **soggetto** [...] dell'Unione approva un piano di cibersicurezza senza indebito ritardo dopo l'istituzione del quadro [...], [...] **l'adozione delle misure di gestione dei rischi** di cibersicurezza [...] **e lo svolgimento della valutazione di maturità e non oltre 21 mesi dopo l'entrata in vigore del presente regolamento**. Il piano **di cibersicurezza** è volto ad aumentare la cibersicurezza complessiva del soggetto **dell'Unione** [...] **interessato** e contribuisce così al [...] rafforzamento di un livello comune elevato di cibersicurezza in tutti i **soggetti** [...] dell'Unione. [...] Il piano **di cibersicurezza** comprende almeno le **misure di gestione dei rischi di cibersicurezza ai sensi dell'articolo 5** [...]. Il piano **di cibersicurezza** è rivisto almeno ogni **due** [...] anni **oppure** a seguito [...] **di ciascuna** valutazione [...] di maturità svolta ai sensi dell'articolo 6 **o di ciascun riesame del quadro ai sensi dell'articolo 4.**

2. [...]

3. Il piano di cibersicurezza **tiene conto** [...] di tutti i documenti di orientamento e di tutte le raccomandazioni applicabili emanati **conformemente all'articolo 13** [...].

4. **Il soggetto dell'Unione sottopone il piano di cibersicurezza, una volta ultimato, all'IICB.**

Articolo 7 bis

Valutazione inter pares

1. L'IICB, su raccomandazione del CERT-UE e previa consultazione dell'ENISA, stabilisce, al più tardi entro ... [24 mesi dopo l'entrata in vigore del presente regolamento], avvalendosi della metodologia per le valutazioni inter pares e della metodologia per l'autovalutazione conformemente all'articolo 16 della direttiva [proposta NIS 2] adeguate, se necessario, alle esigenze dei soggetti dell'Unione, la metodologia e gli aspetti organizzativi di una valutazione inter pares al fine di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità e le politiche degli Stati membri in materia di cibersicurezza necessarie per attuare il presente regolamento. La partecipazione alle valutazioni inter pares è volontaria. I rappresentanti degli Stati membri possono partecipare alla valutazione inter pares in qualità di osservatori. Le valutazioni inter pares sono effettuate da esperti di cibersicurezza assegnati da almeno due soggetti dell'Unione, diversi dai soggetti dell'Unione oggetto della valutazione, e comprendono almeno uno dei seguenti aspetti:

i) il livello di attuazione delle misure di gestione dei rischi di cibersicurezza e degli obblighi di segnalazione di cui agli articoli 5 e 20;

ii) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili;

iii) il livello di attuazione del quadro di condivisione delle informazioni di cui all'articolo 19;

iv) questioni specifiche di natura intersettoriale.

2. I soggetti dell'Unione possono individuare questioni specifiche di cui al paragrafo 1, punto iv), da valutare. La portata della valutazione, comprese le questioni individuate, è comunicata ai soggetti dell'Unione partecipanti prima dell'inizio della valutazione inter pares.

3. Prima dell'inizio di tale valutazione, i soggetti dell'Unione possono effettuare un'autovalutazione degli aspetti valutati e fornire tale autovalutazione agli esperti designati.

4. Le valutazioni inter pares comportano visite in loco reali o virtuali e scambi a distanza. In virtù del principio di buona cooperazione, i soggetti dell'Unione oggetto della valutazione inter pares forniscono agli esperti designati le informazioni necessarie per la valutazione, fatte salve le legislazioni nazionali o dell'Unione in materia di protezione di informazioni sensibili o classificate. Le informazioni ottenute mediante il processo di valutazione inter pares sono utilizzate unicamente a tal fine. Gli esperti che partecipano alla valutazione inter pares non divulgano a terzi le eventuali informazioni sensibili o classificate ottenute nel corso di tale valutazione.

5. Una volta sottoposti a valutazione inter pares, i medesimi aspetti valutati nei soggetti dell'Unione non sono più oggetto di ulteriori valutazioni inter pares in tali soggetti dell'Unione per i due anni successivi alla conclusione della valutazione inter pares, salvo diversamente richiesto dai soggetti dell'Unione o concordato a seguito di una proposta dell'IICB.

6. I soggetti dell'Unione provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti designati siano rivelati agli altri soggetti dell'Unione e all'IICB, prima dell'inizio della valutazione inter pares. I soggetti dell'Unione oggetto della valutazione inter pares possono opporsi alla designazione di determinati esperti per motivi debitamente giustificati comunicati ai soggetti dell'Unione che li designano.

7. Gli esperti che partecipano alle valutazioni inter pares elaborano relazioni sui risultati e sulle conclusioni delle valutazioni. I soggetti dell'Unione sono autorizzati a formulare osservazioni sui rispettivi progetti di relazione, che sono allegati alle relazioni. Le relazioni contengono raccomandazioni per consentire miglioramenti sugli aspetti oggetto della valutazione inter pares. Le relazioni sono presentate all'IICB e alla rete CSIRT, se del caso. I soggetti dell'Unione oggetto della valutazione possono decidere di rendere pubblica la propria relazione o una versione espunta della stessa.

Articolo 8

Attuazione

[...]

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

3. Su richiesta dell'IICB, i soggetti dell'Unione riferiscono in merito a specifici aspetti del 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 dei **soggetti [...] 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:

   a) un rappresentante designato da ciascuno dei seguenti soggetti:

      i) il Parlamento europeo;

      ii) il Consiglio europeo;

      iii) il Consiglio dell'Unione europea;

      iv) la Commissione europea;

      v) la Corte di giustizia dell'Unione europea;

      vi) la Banca centrale europea;

vii) la Corte dei conti europea;

viii) il servizio europeo per l'azione esterna;

ix) il Comitato economico e sociale europeo;

x) il Comitato europeo delle regioni;

xi) la Banca europea per gli investimenti;

xii) il Centro europeo di competenza in materia di cibersicurezza industriale, tecnologica e di ricerca e

xiii) l'Agenzia dell'Unione europea per la cibersicurezza;

b) 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. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3 bis. I membri possono farsi assistere da un supplente. Altri rappresentanti **dei soggetti** [...] sopra elencat**i** o di altri **soggetti** [...] 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 **due** [...] anni. Il supplente del presidente diventa membro a pieno titolo dell'IICB per la stessa durata.

6. L'IICB si riunisce **almeno tre volte all'anno** su iniziativa del presidente, **e/o** su richiesta del CERT-UE **e/**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**, il presidente del gruppo di cooperazione NIS, il presidente della rete EU-CyCLONe e il presidente della rete CSIRT**, o **i loro** [...] supplenti, [...] **possono partecipare** [...] alle riunioni dell'IICB salvo se da questo diversamente deciso **in qualità di osservatori.**

10. **L'ENISA** svolge le funzioni di segretariato dell'IICB [...] **e rende conto al presidente dell'IICB.**

11. I rappresentanti nominati dall'EUAN su proposta del comitato consultivo TIC trasmettono le decisioni dell'IICB **ai membri dell'EUAN** [...]. 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.

[...]

13. L'IICB può **istituire** [...] un comitato esecutivo che lo assista nel suo lavoro e può delegare a tale comitato alcuni dei suoi compiti e poteri**, in particolare quelli di cui all'articolo 10, lettere c) ed e)**. L'IICB stabilisce il regolamento interno del comitato esecutivo, compresi i suoi compiti e i suoi poteri, e il mandato dei suoi membri.

14. Ogni 12 mesi l'IICB presenta al Consiglio una relazione che illustra i progressi compiuti nell'attuazione del presente regolamento e precisa, in particolare, la portata della cooperazione del CERT-UE con i suoi omologhi nazionali in ciascuno degli Stati membri. La relazione costituisce un contributo alla relazione biennale sullo stato della cibersicurezza nell'Unione nello stesso periodo di tempo, conformemente all'articolo 15 della direttiva [proposta NIS 2].

Articolo 10

Compiti dell'IICB

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

a) [...] **monitora e supervisiona in modo efficace l'applicazione** del presente regolamento [...] **e sostiene i soggetti** dell'Unione **per rafforzare la loro cibersicurezza**; **a tal fine, l'IICB può chiedere relazioni ad hoc al CERT-UE e ai soggetti dell'Unione;**

a bis) a seguito di una discussione strategica, adotta una strategia pluriennale volta a innalzare il livello di cibersicurezza nei soggetti dell'Unione, la valuta periodicamente e almeno ogni cinque anni e, ove necessario, la modifica;

b) approva, sulla base di una proposta **presentata dal** [...] 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 **e ogni suo successivo aggiornamento**;

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 [...] gruppi di consulenza tecnica [...] per assistere l'IICB nel suo operato, approva il loro mandato e ne designa i rispettivi presidenti;

j) **adotta documenti di orientamento e raccomandazioni sulla base di una proposta del CERT-UE conformemente all'articolo 13 e chiede al CERT-UE di emanare, ritirare o modificare una proposta relativa a documenti di orientamento o a raccomandazioni, o un invito a intervenire;**

k) riceve e valuta i documenti e le relazioni presentati dai soggetti dell'Unione a norma del presente regolamento;

l) sostiene l'istituzione di un gruppo informale che riunisca i responsabili locali per la cibersicurezza di tutti i soggetti e facilita in tal modo lo scambio di migliori pratiche e informazioni in relazione all'attuazione del presente regolamento;

m) elabora un piano di gestione delle crisi informatiche per sostenere la gestione coordinata degli incidenti gravi a livello operativo che interessano i soggetti dell'Unione e per contribuire allo scambio periodico di informazioni pertinenti, segnatamente riguardo agli impatti e alla gravità degli incidenti gravi e alle possibili modalità di attenuazione.

Articolo 11

Osservanza delle disposizioni

1. L'IICB**, conformemente all'articolo 9, paragrafo 2, e all'articolo 10,** controlla **efficacemente** che **i soggetti** [...] dell'Unione attuino il presente regolamento e i documenti di orientamento, le raccomandazioni e gli inviti a intervenire adottati. **A tale scopo, l'IICB può richiedere le informazioni o la documentazione necessarie per valutare la corretta applicazione delle disposizioni del regolamento da parte dei soggetti dell'Unione. Ai fini dell'adozione delle misure di conformità a norma del presente articolo, il soggetto dell'Unione interessato non ha diritto di voto.**

2. Qualora constati che **i soggetti** [...] 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 del pertinente **soggetto** [...] dell'Unione**, e dopo aver dato al soggetto interessato o alla persona interessata l'opportunità di presentare le proprie opinioni**:

a) emanare un avvertimento **inteso a ovviare alle carenze individuate entro un periodo di tempo specificato, comprese raccomandazioni relative alla modifica dei documenti sulla cibersicurezza adottati dai soggetti dell'Unione sulla base del presente regolamento**; ove necessario, in considerazione di un rischio perentorio per la cibersicurezza, i destinatari dell'avvertimento sono adeguatamente circoscritti;

a bis) emanare una notifica motivata rivolta a un soggetto dell'Unione, qualora le carenze individuate nell'avvertimento precedentemente emanato non siano state sufficientemente affrontate entro un periodo di tempo specificato, e notificare formalmente tale parere al Consiglio, al Parlamento europeo e alla Commissione;

b) **emanare, in particolare:** [...]

i. una raccomandazione relativa allo svolgimento di un audit di un soggetto dell'Unione;

ii. una richiesta relativa allo svolgimento di un audit a cura di un servizio di audit di terzi;

c) chiedere al soggetto dell'Unione di rendere la gestione, la governance e il controllo dei rischi di cibersicurezza conformi alle disposizioni del presente regolamento, se del caso in un modo specificato ed entro un periodo di tempo specificato;

d) emanare un avviso rivolto a tutti gli Stati membri e soggetti dell'Unione che raccomandi la sospensione temporanea dei flussi di dati verso il soggetto dell'Unione.

3. Qualora l'IICB abbia adottato misure a norma del paragrafo 2, lettere da a) a d), il soggetto dell'Unione interessato fornisce un resoconto dettagliato delle misure e azioni adottate per ovviare alle presunte carenze individuate dall'IICB. Il soggetto dell'Unione presenta tale resoconto entro un periodo ragionevole da concordare con l'IICB.

4. Qualora ritenga che vi sia una violazione persistente delle disposizioni del presente regolamento da parte di un soggetto dell'Unione derivante direttamente da azioni o omissioni di un funzionario o altro agente dell'Unione, anche al livello di dirigenza più elevato, l'IICB chiede al soggetto interessato di adottare le misure adeguate, anche di natura disciplinare, conformemente, in particolare, alle norme previste dallo statuto dei funzionari dell'Unione europea e dal regime applicabile agli altri agenti dell'Unione europea. A tal fine, l'IICB trasferisce le informazioni necessarie al soggetto interessato.

Capo IV
CERT-UE

Articolo 12

Missione e compiti del CERT-UE

1. La missione del CERT-UE [...] consiste nel contribuire alla sicurezza dell'ambiente informatico non riservato di tutti [...] **i** soggetti **dell'Unione** 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.

1 bis. Il CERT-UE raccoglie, gestisce, analizza e condivide informazioni con i soggetti dell'Unione sulle minacce, le vulnerabilità e gli incidenti riguardanti le infrastrutture TIC non riservate. Coordina le risposte agli incidenti a livello interistituzionale e a livello di soggetti dell'Unione, anche assicurando o coordinando la prestazione di assistenza operativa specializzata.

2. Il CERT-UE svolge i seguenti compiti per **i soggetti** [...] dell'Unione:

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

b) [...] **offre servizi CSIRT standard per tutti i soggetti dell'Unione attraverso** 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) **sulla base delle informazioni di cui al paragrafo 1 bis,** [...] contribuisce alla consapevolezza situazionale informatica dell'UE **in stretta cooperazione con l'ENISA**. **Tali informazioni sono condivise con l'IICB, oltre che con la rete CSIRT e l'EU-INTCEN;**

f) funge da equivalente del coordinatore designato per i soggetti dell'Unione, di cui all'articolo 6 della direttiva [proposta NIS 2].

[...]

[...]

[...]

[...]

[...]

4. **Nel quadro delle sue competenze,** il CERT-UE avvia una cooperazione strutturata con l'**ENISA** [...] 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 de**i soggetti** [...] 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 de**i soggetti** [...] 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 da**i soggetti** [...] dell'Unione e che cooperano strettamente con tali [...] **soggetti**, 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 **o partecipare a** esercitazioni di cibersicurezza o raccomandare la partecipazione alle esercitazioni esistenti, in stretta cooperazione con l'**ENISA** [...] se del caso, per verificare il livello di cibersicurezza de**i soggetti** [...] dell'Unione.

7. Il CERT-UE può fornire assistenza a**i soggetti** [...] dell'Unione in caso di incidenti in ambienti informatici riservati se [...] **i soggetti dell'Unione** interessat**i** lo richied**ono** esplicitamente**, conformemente alle loro rispettive procedure**. **In tal caso non si applicano le disposizioni di cui agli articoli da 19 a 21 del presente regolamento. La prestazione di assistenza da parte del CERT-UE a norma del presente paragrafo lascia impregiudicate le norme applicabili degli Stati membri o dell'Unione in materia di protezione delle informazioni sensibili o classificate.**

8. Il CERT-UE informa i soggetti dell'Unione delle sue procedure e dei suoi processi di gestione degli incidenti.

9. Il CERT-UE può monitorare il traffico di rete di un soggetto dell'Unione con il consenso del medesimo.

10. Il CERT-UE può, su esplicita richiesta dei dipartimenti politici dei soggetti dell'Unione, fornire consulenza o contributi tecnici su importanti questioni strategiche.

11. Il CERT-UE, in cooperazione con il Garante europeo della protezione dei dati, sostiene i soggetti dell'Unione interessati nell'affrontare gli incidenti che comportano violazioni dei dati personali.

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 [...] i soggetti dell'Unione sono esortati ad adottare entro un termine stabilito. Senza indebito ritardo dopo aver ricevuto l'invito a intervenire, il soggetto dell'Unione interessato informa il CERT-UE delle modalità di applicazione di tali misure;

   b) proposte all'IICB per documenti di orientamento destinati a tutt**i i soggetti** [...] dell'Unione o a una parte di essi;

   c) proposte all'IICB per raccomandazioni destinate a singol**i soggetti** [...] 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 [...] **misure di gestione dei rischi** 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**, compreso un approccio coordinato alla sicurezza della catena di approvvigionamento** [...].

[...]

[...]

Articolo 14

Direttore del CERT-UE

1. La Commissione, dopo aver ottenuto l'approvazione da parte dei due terzi dei membri 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. Il direttore del CERT-UE è responsabile del corretto funzionamento del CERT-UE, nei limiti delle sue attribuzioni e sotto la direzione dell'IICB. È responsabile dell'attuazione della direzione strategica, degli orientamenti, degli obiettivi e delle priorità definiti dall'IICB, nonché della gestione del CERT-UE, incluse le sue risorse finanziarie e umane. Riferisce periodicamente al presidente dell'IICB.

3. Il direttore del CERT-UE assiste l'ordinatore delegato competente nell'elaborazione della relazione annuale di attività contenente informazioni finanziarie e di gestione, compresi i risultati dei controlli, redatta a norma dell'articolo 66, paragrafo 9, del regolamento finanziario, e riferisce periodicamente al medesimo in merito all'attuazione di misure per le quali sono stati subdelegati poteri al direttore del CERT-UE.

4. Il direttore del CERT-UE elabora annualmente una pianificazione finanziaria delle entrate e delle spese amministrative per le sue attività, la proposta di programma di lavoro annuale, la proposta di catalogo dei servizi offerti dal CERT-UE e la relativa revisione, la proposta di modalità degli accordi sul livello dei servizi e la proposta di indicatori essenziali di prestazione per il CERT-UE che devono essere approvati dall'IICB conformemente all'articolo 10.

In sede di revisione dell'elenco dei servizi contenuti nel catalogo dei servizi offerti dal CERT-UE, il direttore del CERT-UE tiene conto delle risorse assegnate al CERT-UE.

5. Il direttore del CERT-UE presenta [...] all'IICB [...] relazioni **annuali** 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, [...] **lettera a)**.

Articolo 15

Questioni finanziarie e relative al personale

[...]

1 bis. Pur essendo istituito come prestatore di servizi interistituzionale autonomo per l'insieme dei soggetti dell'Unione, il CERT-UE è integrato nella struttura amministrativa di una direzione generale della Commissione al fine di beneficiare delle strutture di sostegno amministrativo e alla gestione finanziaria nonché di assistenza contabile della Commissione. La Commissione informa l'IICB in merito alla collocazione amministrativa del CERT-UE e ad eventuali cambiamenti al riguardo. Tale approccio è oggetto di una valutazione periodica, al più tardi prima della fine di qualsiasi quadro finanziario pluriennale istituito a norma dell'articolo 312 TFUE per consentire l'adozione di misure adeguate.

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, [...]4 e 6, e dell'articolo 13, paragrafo 1, [...] **ai soggetti** 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. **I soggetti** [...] 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[13].

5. I costi dei compiti di cui all'articolo 12, paragrafo 5, sono a carico [...] **dei soggetti** dell'Unione che ricevono i servizi del CERT-UE. Le entrate sono destinate alle linee di bilancio che sostengono i costi.

---

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

Articolo 16

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

1. Il CERT-UE coopera e scambia informazioni **senza indebito ritardo** con gli omologhi nazionali degli Stati membri, [...] **in particolare** gli CSIRT **di cui all'articolo 9 della direttiva [proposta NIS 2] e/o se del caso le autorità nazionali competenti** e i punti di contatto unici di cui all'articolo 8 della direttiva [proposta NIS 2] in merito 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 [...] **dei soggetti** dell'Unione, anche tramite la rete CSIRT di cui all'articolo 13 della direttiva [proposta NIS 2].

1 bis. Il CERT-UE informa senza ritardo gli omologhi nazionali pertinenti di cui al paragrafo 1 in uno Stato membro quando viene a conoscenza di incidenti significativi che si verificano nel territorio di tale Stato membro, a meno che il CERT-UE non sappia che il soggetto dell'Unione interessato ha già segnalato tale incidente conformemente all'articolo 20, paragrafo 2 bis.

2. Il CERT-UE**, senza indebito ritardo, scambia** [...] informazioni specifiche su un incidente con gli omologhi nazionali degli Stati membri per facilitare il rilevamento di minacce informatiche o incidenti analoghi **o per contribuire all'analisi di un incidente**, senza **che sia necessario** il consenso [...] **del soggetto dell'Unione** interessato. Il CERT-UE [...] **non scambia** informazioni specifiche su un incidente che rivelino l'identità del bersaglio dell'incidente di cibersicurezza [...] **a meno che:**

   a) vi sia il consenso del soggetto dell'Unione interessato;

   b) il soggetto dell'Unione interessato abbia già comunicato pubblicamente che ne è stato interessato;

c) venga a mancare il consenso del soggetto dell'Unione interessato, ma la pubblicazione dell'identità del soggetto dell'Unione interessato aumenterebbe la probabilità di evitare o attenuare incidenti altrove. Tali decisioni richiedono l'approvazione del direttore del CERT-UE. Il soggetto dell'Unione interessato è informato prima della pubblicazione.

Articolo 17

Cooperazione tra il CERT-UE e <u>altri</u> omologhi [...]

1. Il CERT-UE può cooperare con omologhi [...] **nell'Unione europea diversi da quelli di cui all'articolo 16**, 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, il CERT-UE chiede l'approvazione preventiva dell'IICB **caso per caso**. **Il CERT-UE informa gli omologhi nazionali pertinenti di cui all'articolo 16, paragrafo 1, in uno Stato membro in cui è situato l'omologo, allorché il CERT-UE istituisce una cooperazione con tali omologhi.**

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 **caso per caso**.

3. Il CERT-UE può, **a condizione che sia in vigore un accordo o un contratto di non divulgazione con il partner pertinente,** con il consenso [...] **del soggetto dell'Unione** interessato da un incidente, fornire informazioni in merito all'incidente **specifico** ai partner **di cui ai paragrafi 1 e 2 esclusivamente allo scopo di** [...] contribuire alla sua analisi. **Tali accordi o contratti di non divulgazione sono sottoposti a verifica giuridica in conformità delle pertinenti procedure interne della Commissione. La conclusione di accordi o contratti di non divulgazione non è subordinata alla preventiva approvazione dell'IICB, ma il suo presidente ne è informato.**

4. **In via eccezionale, il CERT-UE può stipulare accordi sul livello dei servizi con soggetti diversi da quelli dell'Unione, previa approvazione dell'IICB.**

Capo V
COOPERAZIONE E OBBLIGHI DI SEGNALAZIONE

Articolo 18
Trattamento delle informazioni

1. Il CERT-UE e [...] **i soggetti** 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[14], compreso l'obbligo, previsto da tale regolamento, di consultare [...] gli altri [...] **soggetti** dell'Unione**, e se del caso gli Stati membri,** qualora la domanda riguardi loro documenti.

[...]

4. Il trattamento delle informazioni da parte del CERT-UE e dei [...] **soggetti** dell'Unione è in linea con le norme **applicabili** [...] sulla sicurezza delle informazioni[...].

[...]

Articolo 19

[...] ***Condivisione delle informazioni sulla cibersicurezza***

-1. I soggetti dell'Unione possono fornire volontariamente al CERT-UE informazioni sulle minacce informatiche, gli incidenti, i quasi incidenti e le vulnerabilità che li interessano. Il CERT-UE garantisce la disponibilità di mezzi di comunicazione efficaci per agevolare la condivisione delle informazioni con i soggetti dell'Unione. Il CERT-UE può trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie.

[14] 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).

1. Per [...] **svolgere la sua missione e i suoi compiti definiti all'articolo 12**, il CERT-UE può chiedere a**i soggetti** [...] dell'Unione di fornirgli informazioni, tratte dai loro rispettivi inventari dei sistemi informatici**, comprese informazioni relative alle minacce informatiche, ai quasi incidenti, alle vulnerabilità, agli indicatori di compromissione, agli allarmi di cibersicurezza e alle raccomandazioni riguardanti la configurazione degli strumenti di cibersicurezza al fine di rilevare gli incidenti informatici** [...]. **Il soggetto** [...] dell'Unione cui è rivolta tale domanda trasmette senza indebito ritardo le informazioni richieste e ogni loro successivo aggiornamento.

2. **I soggetti** [...] 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 **con i soggetti dell'Unione** informazioni specifiche su un incidente che rivelino l'identità de**l soggetto** [...] interessato dall'incidente solo con il consenso di tale soggetto. **Qualora sia negato il consenso, il soggetto interessato fornisce al CERT-UE motivi debitamente giustificati.** [...]

4. Gli obblighi di condivisione non comprendono le informazioni classificate UE ("ICUE") e le informazioni **la cui distribuzione al di fuori del soggetto dell'Unione destinatario sia stata esclusa dalla fonte delle informazioni mediante un contrassegno visibile, a meno che la fonte delle informazioni** [...] **consenta esplicitamente la condivisione di tali informazioni con il CERT-UE.** [...]

Articolo 20

Obblighi di <u>segnalazione</u> [...]

-1. Un incidente è considerato significativo se:

a) ha causato o può causare gravi perturbazioni operative per il funzionamento del soggetto dell'Unione o perdite finanziarie per il soggetto dell'Unione interessato;

b) ha interessato o può interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali.

1. Tutt**i i soggetti** [...] dell'Unione presentano al CERT-UE**:** [...]

[...].

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo sia presumibilmente il risultato di un'azione illegittima o malevola e abbia o possa avere un impatto transfrontaliero;

b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, della sua gravità e del suo impatto, nonché, ove disponibili, gli **indicatori** di compromissione;

c) su richiesta del CERT-UE, una relazione intermedia sui pertinenti aggiornamenti dello status;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente significativo di cui alla lettera b), che comprenda almeno:

i) una descrizione dettagliata dell'incidente significativo, della sua gravità e del suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente significativo;

iii) le misure di attenuazione adottate e in corso;

iv) se del caso, l'impatto transfrontaliero dell'incidente significativo;

e) nei casi di incidenti significativi in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione sullo stato di avanzamento dei lavori in quel momento e una relazione finale entro un mese da quando l'incidente è stato gestito.

[...]

[...]

[...]

[...]

[...]

2 bis. Tutti i soggetti dell'Unione condividono le informazioni comunicate conformemente al paragrafo 1 entro lo stesso termine con ogni omologo nazionale pertinente di cui all'articolo 16, paragrafo 1, nel luogo in cui sono situati.

3. Il CERT-UE trasmette [...] **ogni tre mesi all'IICB, all'EU-INTCEN e alla rete CSIRT** una relazione di sintesi che comprende dati anonimizzati e aggregati sulle minacce informatiche [...], sulle vulnerabilità [...] **conformemente all'articolo 19, sulle risposte dei soggetti dell'Unione agli inviti a intervenire conformemente all'articolo 13, paragrafo 1, lettera a)**, e sugli incidenti significativi notificati conformemente al paragrafo 1. **La relazione costituisce un contributo alla relazione biennale sullo stato della cibersicurezza nell'Unione ai sensi dell'articolo 15 della direttiva [proposta NIS 2].**

4. L'IICB**, entro [6 mesi dall'entrata in vigore del presente regolamento],** [...] **emana** documenti di orientamento o raccomandazioni **che precisano ulteriormente** [...] le modalità**, il formato** e il contenuto della **segnalazione** [...]. **I documenti di orientamento o le raccomandazioni tengono debitamente conto delle disposizioni attuate da qualsiasi atto di esecuzione conformemente all'articolo 20, paragrafo 11, della direttiva [proposta NIS 2].** Il CERT-UE diffonde gli adeguati dettagli tecnici che consentano l'adozione di misure proattive di rilevamento, risposta agli incidenti o attenuazione da parte de**i soggetti** [...] dell'Unione.

5. Gli obblighi di **segnalazione** [...] non comprendono le ICUE e le informazioni **la cui distribuzione al di fuori del soggetto dell'Unione destinatario sia stata esclusa dalla fonte delle informazioni mediante un contrassegno visibile, a meno che la fonte delle informazioni** [...] **consenta esplicitamente la condivisione di tali informazioni con il CERT-UE.** [...]

Articolo 21

Coordinamento della risposta in caso di incidenti e cooperazione [...]

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:

   a) **i soggetti** [...] dell'Unione;

   b) gli omologhi di cui agli articoli 16 e 17.

2. Il CERT-UE**,** [...] **se del caso in stretta cooperazione con l'ENISA conformemente all'articolo 7, paragrafo 7, lettera d), del regolamento sulla cibersicurezza[15],** facilita il coordinamento fra **i soggetti** [...] dell'Unione in materia di risposta agli incidenti, anche tramite:

   a) il contributo a una comunicazione esterna coerente;

   [...]

   c) l'uso ottimale delle risorse operative;

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

3. Il CERT-UE**, in stretta cooperazione con l'ENISA,** sostiene **i soggetti** [...] dell'Unione per quanto riguarda la consapevolezza situazionale delle minacce informatiche, delle vulnerabilità e degli incidenti.

---

15 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").

4. L'IICB**, entro [12 mesi dalla data di entrata in vigore del presente regolamento], sulla base di una proposta del CERT-UE, adotta** [...] **documenti di** orientamento **o raccomandazioni** 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

Gestione degli incidenti [...] *grav**i***

-1. Al fine di sostenere la gestione coordinata degli incidenti gravi a livello operativo che interessano i soggetti dell'Unione e per contribuire allo scambio periodico di informazioni pertinenti tra i soggetti dell'Unione e con gli Stati membri, l'IICB elabora un piano di gestione delle crisi informatiche basato sulle attività di cui all'articolo 21, paragrafo 2, in stretta cooperazione con il CERT-UE e l'ENISA, che comprende almeno i seguenti elementi:

a) le modalità del coordinamento e del flusso di informazioni tra i soggetti dell'Unione per la gestione degli incidenti gravi a livello operativo;

b) procedure operative standard comuni;

c) una tassonomia comune della gravità degli incidenti gravi e dei punti di innesco delle crisi;

d) esercitazioni periodiche;

e) canali di comunicazione sicuri da utilizzare;

f) un punto di contatto per EU-CyCLONe, che condivide le informazioni pertinenti con EU-CyCLONe quali contributi alla conoscenza situazionale condivisa.

1. Il CERT-UE coordina, fra **i soggetti** [...] dell'Unione, le risposte agli **incidenti** [...] gravi e tiene un inventario delle competenze tecniche che risulterebbero necessarie per la risposta agli incidenti in caso di **incidenti gravi** [...].

2. **I soggetti** [...] 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. A seguito di specifica richiesta da parte di uno Stato membro in cui è situato il soggetto dell'Unione interessato e [...] con l'accordo **del soggetto** [...] dell'Unione interessat**o**, il CERT-UE può anche rivolgersi agli esperti dell'elenco di cui al paragrafo 2 per contribuire alla risposta a un **incidente** [...] grave in **tale soggetto dell'Unione** [...].

Capo VI
DISPOSIZIONI FINALI

Articolo 23

Riassegnazione di bilancio iniziale

La Commissione propone la riassegnazione di personale e risorse finanziarie da**i** pertinenti **soggetti** [...] 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 **riesaminare il** [...] presente regolamento.

2. La Commissione riferisce al Parlamento europeo e al Consiglio in merito all'attuazione del presente regolamento entro **36** [...] 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 **entro** [...] cinque anni dalla data di entrata in vigore. **La relazione, se necessario, è corredata di una proposta legislativa.**

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*
Il presidente / La presidente	*Il presidente*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ALLEGATO II

[...]

[...]

[...]

[...]

[...]

[...]

[...]