UNIONE EUROPEA

IL PARLAMENTO EUROPEO **IL CONSIGLIO**

Strasburgo, 13 dicembre 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

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

REGOLAMENTO (UE, Euratom) 2023/…
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 13 dicembre 2023

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

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[1],

[1] Posizione del Parlamento europeo del 21 novembre 2023 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio dell'8 dicembre 2023.

considerando quanto segue:

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

(2) Il panorama delle minacce informatiche che pesano sui 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 all'indebolimento delle infrastrutture digitali. Il ritmo di perpetrazione degli attacchi informatici da parte degli autori delle minacce 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 TIC dei 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 solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione. Inoltre, alcuni ambienti TIC dei soggetti dell'Unione sono connessi con gli ambienti TIC degli Stati membri, e un incidente in un soggetto dell'Unione può rappresentare un rischio per la cibersicurezza degli ambienti TIC degli Stati membri e viceversa. La condivisione di informazioni specifiche su un incidente può 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 ad affrontare sia autori di minacce molto esperti e dotati di risorse adeguate, sia altri tipi di minacce. Al tempo stesso, fra tali soggetti il livello e la maturità della ciberresilienza e la capacità di individuare e contrastare attività informatiche dolose variano in modo significativo. Ai fini del loro funzionamento, è quindi necessario che i soggetti dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso l'attuazione di misure di gestione dei rischi di cibersicurezza commisurate ai rischi per la cibersicurezza individuati, lo scambio di informazioni e la collaborazione.

(5) La direttiva (EU) 2022/2555 del Parlamento europeo e del Consiglio[1] è volta a migliorare ulteriormente le ciberresilienza e la capacità di risposta agli incidenti di soggetti pubblici e privati, delle autorità e degli organi competenti così come dell'Unione nel suo complesso. È pertanto necessario che i soggetti dell'Unione agiscano in tal senso prevedendo norme che siano coerenti con la direttiva (UE) 2022/2555 e rispecchino il suo livello di ambizione.

(6) Per raggiungere un livello comune elevato di cibersicurezza, è necessario che ogni soggetto dell'Unione istituisca un quadro interno di gestione, governance e controllo dei rischi per la cibersicurezza ("quadro"), che garantisca una gestione efficace e prudente di tutti i rischi per la cibersicurezza e tenga conto della continuità operativa e della gestione delle crisi. Il quadro dovrebbe stabilire politiche in materia di cibersicurezza, comprensive di obiettivi e priorità, per la sicurezza dei sistemi informativi e di rete che costituiscono la totalità dell'ambiente TIC non riservato. Il quadro dovrebbe basarsi su un approccio multirischio che miri a proteggere i sistemi informativi 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 ai loro impianti di trattamento delle informazioni 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 informativi e di rete.

---

[1] Direttiva (EU) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

(7) Per gestire i rischi per la cibersicurezza individuati nell'ambito del quadro, ciascun soggetto dell'Unione dovrebbe adottare misure tecniche, operative e organizzative adeguate e proporzionate. Tali misure dovrebbero riguardare i settori e le misure di gestione dei rischi per la cibersicurezza previsti dal presente regolamento per rafforzare la cibersicurezza di ciascun soggetto dell'Unione.

(8) Le risorse e i rischi per la cibersicurezza individuati nel quadro nonché le conclusioni tratte dalle valutazioni di maturità periodiche della cibersicurezza dovrebbero essere rispecchiate in un piano di cibersicurezza stabilito da ciascun soggetto dell'Unione. Il piano di cibersicurezza dovrebbe includere le misure di gestione dei rischi per la cibersicurezza adottate.

(9) Poiché garantire la cibersicurezza è un processo continuo, l'adeguatezza e l'efficacia delle misure adottate a norma del presente regolamento dovrebbero essere riviste periodicamente alla luce dell'evoluzione dei rischi per la cibersicurezza, delle risorse e della maturità in materia di cibersicurezza dei soggetti dell'Unione. Il quadro dovrebbe essere riesaminato periodicamente e almeno ogni quattro anni, mentre il piano di cibersicurezza dovrebbe essere rivisto ogni due anni o più spesso, se necessario, a seguito delle valutazioni della maturità in materia di cibersicurezza o di ciascun riesame sostanziale del quadro.

(10) Le misure di gestione dei rischi per la cibersicurezza messe in atto dai soggetti dell'Unione dovrebbero prevedere politiche volte, ove possibile, a rendere trasparente il codice sorgente, tenendo conto delle garanzie per i diritti di terzi o dei soggetti dell'Unione. Tali politiche dovrebbero essere proporzionate al rischio per la cibersicurezza e sono intese a facilitare l'analisi delle minacce informatiche, senza creare obblighi di comunicazione o diritti di accesso al codice di terzi oltre i termini contrattuali applicabili.

(11) Gli strumenti e le applicazioni di cibersicurezza open source possono contribuire a un livello più elevato di apertura. Gli standard aperti facilitano l'interoperabilità tra gli strumenti di sicurezza, a vantaggio della sicurezza dei portatori di interessi. Gli strumenti e le applicazioni open source in materia di cibersicurezza possono mobilitare la più ampia comunità di sviluppatori, consentendo la diversificazione dei fornitori. Una fonte aperta può portare a un processo di verifica più trasparente degli strumenti connessi alla cibersicurezza e a un processo di individuazione delle vulnerabilità guidato dalla comunità. I soggetti dell'Unione dovrebbero pertanto poter promuovere l'utilizzo di software open source e standard aperti, perseguendo politiche relative all'uso di dati aperti e open source come parte della sicurezza attraverso la trasparenza.

(12) Le differenze esistenti fra i soggetti dell'Unione richiedono flessibilità nell'attuazione del presente regolamento. Le misure per un livello comune elevato di cibersicurezza previste dal presente regolamento 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 dovrebbero pertanto istituire i propri quadri e dovrebbero adottare le proprie misure di gestione dei rischi per la cibersicurezza e i propri piani 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 della cooperazione tra i soggetti dell'Unione e tra i soggetti dell'Unione e le controparti degli Stati membri.

(13) Al fine di ottimizzare l'uso delle risorse, il presente regolamento dovrebbe prevedere la possibilità che due o più soggetti dell'Unione con strutture simili cooperino nell'esecuzione delle valutazioni della maturità in materia di cibersicurezza per i loro rispettivi soggetti.

(14) 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 per la cibersicurezza corso dal sistema informativo 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 relativo alle TIC per migliorare il livello di cibersicurezza. A lungo termine dovrebbe essere perseguito un obiettivo indicativo dell'ordine di almeno il 10 %. La valutazione della maturità in materia di cibersicurezza dovrebbe determinare se la spesa per la cibersicurezza del soggetto dell'Unione sia proporzionata ai rischi per la cibersicurezza cui quest'ultimo è esposto. Fatte salve le norme relative al bilancio annuale dell'Unione a norma dei trattati, nella proposta per il primo bilancio annuale da adottare dopo l'entrata in vigore del presente regolamento la Commissione dovrebbe tenere conto degli obblighi derivanti dal presente regolamento nel valutare il fabbisogno di bilancio e di personale dei soggetti dell'Unione risultante dai loro stati di previsione delle spese.

(15) 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 del soggetto dell'Unione dovrebbe essere responsabile dell'attuazione del presente regolamento, anche per quanto riguarda l'istituzione del quadro, l'adozione delle misure di gestione dei rischi di cibersicurezza e l'approvazione del piano di cibersicurezza. Occuparsi della cultura della cibersicurezza, ossia della pratica quotidiana della cibersicurezza, è parte integrante del quadro e delle corrispondenti misure di gestione dei rischi per la cibersicurezza in tutti i soggetti dell'Unione.

(16) La sicurezza dei sistemi informativi e di rete che trattano informazioni classificate UE (ICUE) è essenziale. I soggetti dell'Unione che trattano ICUE sono tenuti ad applicare i quadri normativi completi in vigore per la protezione di tali informazioni, compresi specifici meccanismi di governance, politiche e procedure di gestione dei rischi. È necessario che i sistemi informativi e di rete che trattano ICUE rispettino norme di sicurezza più rigorose rispetto ai sistemi d'informazione e di rete non classificati. Pertanto, i sistemi informativi e di rete che trattano ICUE sono più resilienti alle minacce e agli incidenti informatici. Di conseguenza, pur riconoscendo la necessità di un quadro comune al riguardo, il presente regolamento non dovrebbe applicarsi ai sistemi informativi e di rete che trattano ICUE. Tuttavia, se esplicitamente richiesto da un soggetto dell'Unione, la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (CERT-UE) dovrebbe poter fornire assistenza a tale soggetto dell'Unione in relazione a incidenti in ambienti TIC classificati.

(17) I soggetti dell'Unione dovrebbero valutare i rischi per la cibersicurezza legati alle relazioni con i fornitori e i prestatori di servizi, compresi i prestatori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti, e dovrebbero adottare misure adeguate per affrontarli. Le misure di cibersicurezza dovrebbero essere ulteriormente specificate in indirizzi o raccomandazioni emanati dal CERT-UE. Nel definire le misure e gli indirizzi dovrebbero essere presi in debita considerazione lo stato delle conoscenze e, se del caso, le pertinenti norme europee e internazionali nonché le normative e politiche rilevanti dell'Unione, comprese le valutazioni dei rischi per la cibersicurezza e le raccomandazioni emanate dal gruppo di cooperazione istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555, come la valutazione dei rischi della cibersicurezza delle reti 5G coordinata a livello dell'UE e il pacchetto di strumenti dell'UE per la cibersicurezza del 5G. Tenuto conto del panorama delle minacce e dell'importanza di consolidare la ciberresilienza per i soggetti dell'Unione, potrebbe essere inoltre richiesta la certificazione di prodotti, servizi e processi TIC nell'ambito di specifici sistemi europei di certificazione della cibersicurezza adottati conformemente all'articolo 49 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[1].

[1] 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).

(18) Nel maggio 2011 i segretari generali delle istituzioni e degli organi dell'Unione hanno deciso di istituire un gruppo per la preconfigurazione del CERT-UE, posto 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 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[1]. 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.

(19) Il CERT-UE dovrebbe essere rinominato servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione, ma dovrebbe mantenere il nome abbreviato CERT-UE a fini di riconoscibilità del nome.

---

[1] Accordo tra il Parlamento europeo, il Consiglio europeo, il Consiglio dell'Unione europea, la Commissione europea, la Corte di giustizia dell'Unione europea, la Banca centrale europea, la Corte dei conti europea, il Servizio europeo per l'azione esterna, il Comitato economico e sociale europeo, il Comitato europeo delle regioni e la Banca europea per gli investimenti sull'organizzazione e il funzionamento della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE) (GU C 12 del 13.1.2018, pag. 1).

(20) Oltre a conferire maggiori compiti e un ruolo più ampio al CERT-UE, il presente regolamento istituisce il comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board* – IICB) al fine di contribuire all'instaurarsi di un livello comune elevato di cibersicurezza tra i soggetti dell'Unione. L'IICB dovrebbe svolgere un ruolo esclusivo nel vigilare e sostenere l'attuazione del presente regolamento da parte dei soggetti dell'Unione e nel vigilare sull'attuazione delle priorità e degli obiettivi generali da parte del CERT-UE nonché nel fornire a tale centro di una direzione strategica. L'IICB dovrebbe pertanto garantire la rappresentanza delle istituzioni dell'Unione e includere rappresentanti degli organi e degli organismi dell'Unione attraverso la rete delle agenzie dell'Unione europea (*EU Agencies Network* – EUAN). L'organizzazione e il funzionamento dell'IICB dovrebbero essere ulteriormente disciplinati da un 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 dovrebbe poter 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 controllo della loro attuazione. L'IICB dovrebbe stabilire il regolamento interno del comitato esecutivo, compresi i suoi compiti e i suoi poteri.

(21) L’IICB mira a sostenere i soggetti dell’Unione nell’incrementare le rispettive posizioni di cibersicurezza mediante l’attuazione del presente regolamento. Al fine di sostenere i soggetti dell’Unione, l’IICB dovrebbe fornire orientamenti al direttore del CERT-UE, adottare una strategia pluriennale per innalzare il livello di cibersicurezza nei soggetti dell’Unione, stabilire la metodologia e altri aspetti delle valutazioni inter pares volontarie e facilitare l’istituzione di un gruppo informale di responsabili locali della cibersicurezza, con il sostegno dell’Agenzia dell’Unione europea per la cibersicurezza (ENISA), al fine di scambiare migliori pratiche e informazioni in relazione all’attuazione del presente regolamento.

(22) Al fine di conseguire un livello elevato di cibersicurezza in tutti i soggetti dell'Unione, gli interessi degli organi e degli organismi dell'Unione che gestiscono il proprio ambiente TIC dovrebbero essere rappresentati nell'IICB da tre rappresentanti designati dall'EUAN. La sicurezza del trattamento dei dati personali, e quindi anche la loro cibersicurezza, è un elemento fondamentale della protezione dei dati. Alla luce delle sinergie tra la protezione dei dati e la cibersicurezza, il garante europeo della protezione dei dati dovrebbe essere rappresentato in seno all'IICB in qualità di soggetto dell'Unione assoggettato al presente regolamento, con competenze specifiche nel settore della protezione dei dati, compresa la sicurezza delle reti di comunicazione elettronica. Data l'importanza dell'innovazione e della competitività nella cibersicurezza, il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza dovrebbe essere rappresentato in seno all'IICB. In considerazione del ruolo dell'ENISA quale centro di competenze in materia di cibersicurezza e del sostegno fornito dall'ENISA, e in considerazione dell'importanza della cibersicurezza delle infrastrutture e dei servizi spaziali dell'Unione, l'ENISA e l'Agenzia dell'Unione europea per il programma spaziale dovrebbero essere rappresentate in seno all'IICB. Alla luce del ruolo assegnato al CERT-UE a norma del presente regolamento, il direttore del CERT-UE dovrebbe essere invitato dal presidente dell'IICB a tutte le riunioni dell'IICB, tranne quando l'IICB discute di questioni direttamente connesse al direttore del CERT-UE.

(23) L’IICB dovrebbe controllare l’osservanza del presente regolamento come pure l’attuazione degli indirizzi e delle raccomandazioni nonché degli inviti a intervenire. L’IICB dovrebbe essere coadiuvato sulle questioni tecniche da gruppi di consulenza tecnica composti come da esso ritenuto utile. I gruppi di consulenza tecnica dovrebbero lavorare in stretta collaborazione con il CERT-UE, con i soggetti dell'Unione e con altri portatori di interessi a seconda delle necessità.

(24) Qualora constati che un soggetto dell'Unione non ha attuato efficacemente il presente regolamento o gli indirizzi, le raccomandazioni o gli inviti a intervenire emanati in base ad esso, l'IICB, ferme restando le procedure interne del soggetto dell'Unione interessato, dovrebbe poter procedere con le misure di conformità. L'IICB dovrebbe applicare le misure di conformità progressivamente, vale a dire che dovrebbe innanzitutto adottare la misura meno severa, vale a dire un parere motivato, e solo se necessario adottare misure sempre più severe, culminando nella misura più grave, vale a dire una raccomandazione di sospensione temporanea dei flussi di dati verso il soggetto dell'Unione interessato. Tale raccomandazione dovrebbe essere applicata solo in casi eccezionali di violazioni ripetute nel tempo, deliberate, ripetute o gravi del presente regolamento da parte del soggetto dell'Unione interessato.

(25) Il parere motivato rappresenta la misura di conformità meno severa per colmare le lacune osservate nell'attuazione del presente regolamento. L'IICB dovrebbe essere in grado di dare seguito a un parere motivato con orientamenti che aiutino il soggetto dell'Unione a garantire che il suo quadro, le sue misure di gestione dei rischi di cibersicurezza, il suo piano di cibersicurezza e le sue segnalazioni siano conformi al presente regolamento e successivamente emanando un avvertimento per affrontare le carenze individuate del soggetto dell'Unione entro un periodo specificato. Se le carenze individuate nell'avvertimento non sono state affrontate in misura sufficiente, l'IICB dovrebbe essere in grado di emanare una notifica motivata.

(26) L'IICB dovrebbe essere in grado di raccomandare lo svolgimento di un audit di un soggetto dell'Unione. A tal fine, il soggetto dell'Unione dovrebbe poter utilizzare la propria funzione di audit interno. L'IICB dovrebbe inoltre essere in grado di 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.

(27) In casi eccezionali di inosservanza a lungo termine, deliberata, ripetuta o grave del presente regolamento da parte di un soggetto dell'Unione, l'IICB dovrebbe essere in grado di raccomandare a tutti gli Stati membri e ai soggetti dell'Unione, come misura di ultima istanza, una sospensione temporanea dei flussi di dati verso il soggetto dell'Unione fino alla cessazione dell'inosservanza da parte del soggetto interessato. Tale raccomandazione dovrebbe essere comunicata tramite canali di comunicazione adeguati e sicuri.

(28) Per garantire la corretta attuazione del presente regolamento, qualora ritenga che una violazione persistente del presente regolamento da parte di un soggetto dell'Unione sia direttamente imputabile ad azioni od omissioni di un membro del personale, anche al livello di dirigenza più elevato, l'IICB dovrebbe chiedere al soggetto dell'Unione interessato di adottare misure adeguate, compresa la richiesta di prendere in considerazione l'adozione di misure di natura disciplinare, conformemente alle norme e alle procedure previste dallo statuto dei funzionari dell'Unione europea e dal regime applicabile agli altri agenti dell'Unione, stabilito dal regolamento (CEE, Euratom, CECA) n. 259/68[1] del Consiglio ("statuto dei funzionari"), nonché a qualsiasi altra norma e procedura applicabile.

(29) Il CERT-UE dovrebbe contribuire alla sicurezza dell'ambiente TIC 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 che gli sono attribuiti a norma del presente regolamento. Il CERT-UE dovrebbe fungere, per i soggetti dell'Unione, da equivalente del coordinatore designato ai fini della divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555.

---

[1] Regolamento (CEE, Euratom, CECA) 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, ed istituisce speciali misure applicabili temporaneamente ai funzionari della Commissione (GU L 56 del 4.3.1968, pag. 1).

(30) Il CERT-UE dovrebbe sostenere l'attuazione delle misure per un livello comune elevato di cibersicurezza proponendo all'IICB indirizzi e raccomandazioni ed emanando inviti a intervenire. Tali indirizzi e raccomandazioni dovrebbero essere approvati dall'IICB. Ove necessario, il CERT-UE dovrebbe emanare inviti a intervenire che descrivano le misure di sicurezza urgenti che i soggetti dell'Unione sono esortati ad adottare entro un termine stabilito. L'IICB dovrebbe chiedere al CERT-UE di emanare, ritirare o modificare una proposta di indirizzi o raccomandazioni o un invito a intervenire.

(31) Il CERT-UE dovrebbe inoltre svolgere il ruolo ad esso assegnato nella direttiva (UE) 2022/2555 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 (*the computer security incident response teams* – CSIRT) istituita a norma dell'articolo 15 di tale direttiva. Inoltre, in linea con la raccomandazione (EU) 2017/1584 della Commissione[1] il CERT-UE dovrebbe cooperare e coordinare una risposta con i portatori di interessi. Per contribuire a un livello comune elevato di cibersicurezza nell'Unione, il CERT-UE dovrebbe condividere con gli omologhi degli Stati membri informazioni specifiche sugli incidenti. Il CERT-UE dovrebbe inoltre collaborare con altri omologhi pubblici e privati, anche in seno all'Organizzazione del trattato del Nord Atlantico, previa approvazione da parte dell'IICB.

---

[1] 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).

(32) Nel sostenere la cibersicurezza operativa, il CERT-UE dovrebbe avvalersi delle competenze disponibili dell'ENISA attraverso la cooperazione strutturata di cui al regolamento (UE) 2019/881. Se del caso, dovrebbero essere conclusi appositi accordi tra le due entità 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'ENISA la sua relazione sul panorama delle minacce.

(33) Il CERT-UE dovrebbe essere in grado di cooperare e scambiare informazioni con le pertinenti comunità della cibersicurezza nell'Unione e nei suoi Stati membri per promuovere la cooperazione operativa e consentire alle reti esistenti di realizzare appieno il loro potenziale di protezione dell'Unione.

(34) Poiché i servizi e i compiti del CERT-UE sono svolti nell'interesse dei soggetti dell'Unione, ogni soggetto dell'Unione che sostenga spese per le TIC dovrebbe contribuire con una quota equa a tali servizi e compiti. Tali contributi non pregiudicano l'autonomia di bilancio dei soggetti dell'Unione.

(35) 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 e di ripresa dopo eventuali incidenti, i soggetti dell'Unione dovrebbero poter notificare al CERT-UE gli incidenti, le minacce informatiche, le vulnerabilità e i quasi incidenti e condividere adeguati dettagli tecnici che consentano di rilevare o attenuare e di rispondere a incidenti, minacce informatiche, vulnerabilità e quasi incidenti analoghi in altri soggetti dell'Unione. Seguendo lo stesso approccio della direttiva (UE) 2022/2555, i soggetti dell'Unione dovrebbero essere tenuti a presentare un preallarme al CERT-UE entro 24 ore dal momento in cui vengono a conoscenza di un incidente significativo. 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 TIC dei soggetti dell'Unione e quelli degli omologhi dei soggetti dell'Unione contro incidenti analoghi.

(36) 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 e contribuisca ad aumentare la loro posizione di cibersicurezza complessiva. A tale proposito, il presente regolamento dovrebbe includere la segnalazione di incidenti che, sulla base di una valutazione iniziale condotta dal soggetto dell'Unione interessato, potrebbero causare gravi perturbazioni operative per il funzionamento del soggetto dell'Unione interessato 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 informativi 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.

(37) Poiché l'infrastruttura e i sistemi informativi e di rete del pertinente soggetto dell'Unione e dello Stato membro in cui è situato tale soggetto dell'Unione sono interconnessi, 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 gli omologhi pertinenti dello Stato membro, designati o istituiti a norma degli articoli 8 e 10 della direttiva (UE) 2022/2555, del verificarsi di un incidente significativo in merito al quale effettua una segnalazione al CERT-UE. Quando viene a conoscenza di un incidente significativo all'interno di uno Stato membro, il CERT-UE ne dovrebbe informare gli omologhi pertinenti in quello Stato membro.

(38) 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. Il rappresentante della Commissione in seno all'IICB dovrebbe, subordinatamente al piano di gestione delle crisi informatiche, fungere da punto di contatto per facilitare la condivisione da parte dell'IICB delle pertinenti informazioni riguardanti gli incidenti gravi con la rete europea delle organizzazioni di collegamento per le crisi informatiche (*European cyber crisis liaison organisation network* – EU-CyCLONe), quale contributo alla condivisione della conoscenza situazionale. Il ruolo del rappresentante della Commissione in seno all'IICB quale punto di contatto non dovrebbe pregiudicare il ruolo separato e distinto della Commissione nell'ambito di EU-CyCLONe a norma dell'articolo 16, paragrafo 2, della direttiva (UE) 2022/2555.

(39) Il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[1] si applica a qualunque trattamento dei dati personali a norma del presente regolamento. Il trattamento dei dati personali potrebbe riguardare le misure adottate nell'ambito della gestione dei rischi di cibersicurezza, della gestione della vulnerabilità e degli incidenti, della condivisione di informazioni sugli incidenti, delle minacce informatiche e delle vulnerabilità, nonché del coordinamento e della cooperazione in materia di risposta agli incidenti. Tali misure potrebbero richiedere il trattamento di determinate categorie di dati personali, quali gli indirizzi IP, i localizzatori uniformi di risorse (URL), i nomi di dominio, gli indirizzi di posta elettronica, i ruoli organizzativi dell'interessato, le marcature temporali, gli oggetti delle e-mail o i nomi dei file. Tutte le misure adottate a norma del presente regolamento dovrebbero essere conformi al quadro in materia di protezione dei dati e tutela della vita privata. I soggetti dell'Unione, il CERT-UE e, se del caso, l'IICB dovrebbero adottare tutte le pertinenti misure tecniche e organizzative di salvaguardia per garantire tale conformità in modo responsabile.

(40) Il presente regolamento stabilisce la base giuridica per il trattamento dei dati personali da parte dei soggetti dell'Unione, del CERT-UE e, se del caso, dell'IICB, ai fini dello svolgimento dei loro compiti e dell'adempimento dei loro obblighi a norma del presente regolamento, conformemente all'articolo 5, paragrafo 1, lettera b), del regolamento (UE) 2018/1725. Il CERT-UE può agire in qualità di responsabile del trattamento o titolare del trattamento a seconda dei compiti svolti a norma del regolamento (UE) 2018/1725.

---

[1] 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).

(41) In alcuni casi, per adempiere ai loro obblighi previsti dal presente regolamento di garantire un livello elevato di cibersicurezza, in particolare nel contesto della gestione delle vulnerabilità e degli incidenti, può essere necessario che i soggetti dell'Unione e il CERT-UE trattino categorie particolari di dati personali di cui all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725. Il presente regolamento stabilisce la base giuridica per il trattamento di categorie particolari di dati personali da parte dei soggetti dell'Unione e del CERT-UE conformemente all'articolo 10, paragrafo 2, lettera g), del regolamento (UE) 2018/1725. Il trattamento di categorie particolari di dati personali a norma del presente regolamento dovrebbe essere rigorosamente proporzionato all'obiettivo perseguito. Fatte salve le condizioni di cui all'articolo 10, paragrafo 2, lettera g), di tale regolamento, i soggetti dell'Unione e il CERT-UE dovrebbero essere in grado di trattare tali dati solo nella misura necessaria e ove esplicitamente previsto dal presente regolamento. Nel trattare categorie particolari di dati personali, i soggetti dell'Unione e il CERT-UE dovrebbero rispettare l'essenza del diritto alla protezione dei dati e prevedere misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati.

(42) A norma dell'articolo 33 del regolamento (UE) 2018/1725, i soggetti dell'Unione e il CERT-UE, tenendo conto dello stato delle conoscenze e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, dovrebbero mettere in atto misure tecniche e organizzative adeguate per garantire un adeguato livello di sicurezza dei dati personali, tra cui la concessione di diritti di accesso limitati in base al principio della necessità di conoscere, l'applicazione dei principi della traccia di audit, l'adozione della catena di custodia, la conservazione dei dati a riposo in un ambiente controllato e verificabile, procedure operative standardizzate e misure di tutela della vita privata quali la pseudonimizzazione o la cifratura. Tali misure non dovrebbero essere attuate in modo tale da compromettere le finalità di gestione degli incidenti e l'integrità delle prove. Qualora un soggetto dell'Unione o il CERT-UE trasferisca dati personali relativi a un incidente, comprese categorie particolari di dati personali, a una controparte o a un partner ai fini del presente regolamento, tali trasferimenti dovrebbero essere conformi al regolamento (UE) 2018/1725. In caso di trasferimento a terzi di categorie particolari di dati personali, i soggetti dell'Unione e il CERT-UE dovrebbero garantire che il terzo applichi misure di protezione dei dati personali di livello equivalente a quello previsto dal regolamento (UE) 2018/1725.

(43) I dati personali trattati ai fini del presente regolamento dovrebbero essere conservati solo per il periodo di tempo necessario, conformemente al regolamento (UE) 2018/1725. I soggetti dell'Unione e, se del caso, il CERT-UE che agisce in qualità di titolare del trattamento dovrebbero fissare periodi di conservazione limitati a quanto necessario per conseguire le finalità specificate. Per quanto riguarda, in particolare, i dati personali raccolti per il trattamento degli incidenti, i soggetti dell'Unione e il CERT-UE dovrebbero distinguere tra i dati personali raccolti per individuare una minaccia informatica nei loro ambienti TIC al fine di prevenire un incidente e i dati personali raccolti ai fini della mitigazione, della risposta e del recupero in caso di incidente. Per l'individuazione di una minaccia informatica, è importante tenere conto del periodo di tempo durante il quale il responsabile di una minaccia può passare inosservato all'interno di un sistema. Ai fini della mitigazione, della risposta e del recupero in caso di incidente, è importante valutare se i dati personali siano necessari per rintracciare e gestire un incidente ricorrente o un incidente di natura analoga per il quale possa essere dimostrata una correlazione.

(44) Il trattamento delle informazioni da parte dei soggetti dell'Unione e del CERT-UE dovrebbe essere conforme alle norme applicabili sulla sicurezza delle informazioni. L'inclusione della sicurezza delle risorse umane come misura di gestione dei rischi di cibersicurezza dovrebbe essere anch'essa conforme alle norme applicabili.

(45) 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 strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i CSIRT e in alcuni centri di analisi e condivisione delle informazioni.

(46) Il presente regolamento dovrebbe essere oggetto di una valutazione periodica alla luce dei futuri negoziati dei quadri finanziari pluriennali, in modo da consentire l'adozione di ulteriori decisioni in relazione al funzionamento e al ruolo istituzionale del CERT-UE, inclusa la possibile istituzione del CERT-UE come organismo dell'Unione.

(47) 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. La relativa relazione, con il contributo dell'IICB, dovrebbe valutare l'opportunità di includere i sistemi informativi e di rete che trattano ICUE nell'ambito di applicazione del presente regolamento, in particolare in assenza di norme in materia di sicurezza delle informazioni comuni ai soggetti dell'Unione.

(48) In ottemperanza al principio di proporzionalità, per realizzare l'obiettivo fondamentale del raggiungimento di un livello comune elevato di cibersicurezza nei soggetti dell'Unione, è necessario e opportuno istituire norme sulla cibersicurezza per i soggetti dell'Unione. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo, in conformità dell'articolo 5, paragrafo 4, del trattato sull'Unione europea.

(49) Il presente regolamento riflette il fatto che i soggetti dell'Unione differiscono per dimensioni e capacità, anche in termini di risorse finanziarie e umane.

(50) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 17 maggio 2022[1],

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

[1] GU C 258 del 5.7.2022, pag. 10.

Capo I
Disposizioni generali

Articolo 1

Oggetto

Il presente regolamento stabilisce misure volte a conseguire un livello comune elevato di cibersicurezza nei soggetti dell'Unione con riferimento:

a) alla definizione da parte di ciascun soggetto dell'Unione di un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza a norma dell'articolo 6;

b) alla gestione e alla segnalazione dei rischi per la cibersicurezza e alla condivisione delle informazioni;

c) all'organizzazione, al funzionamento e all'operatività del comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10, nonché all'organizzazione, al funzionamento e all'operatività del servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione (CERT-UE);

d) al controllo dell'attuazione del presente regolamento.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica ai soggetti dell'Unione, al comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10 e al CERT-UE.

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

3. Ad eccezione dell'articolo 13, paragrafo 8, il presente regolamento non si applica ai sistemi informativi 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 (TFUE), dal trattato che istituisce la Comunità europea dell'energia atomica, oppure a norme degli stessi;

2) "sistema informativo e di rete": un sistema informativo e di rete quale definito all'articolo 6, punto 1), della direttiva (UE) 2022/2555;

3) "sicurezza dei sistemi informativi e di rete": la sicurezza dei sistemi informativi e di rete quale definita all'articolo 6, punto 2), della direttiva (UE) 2022/2555;

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 un organo di coordinamento e sorveglianza responsabile del funzionamento di un soggetto dell'Unione, al livello amministrativo più alto, con il mandato di adottare o autorizzare decisioni in linea con i sistemi di governance ad alto livello di tale soggetto dell'Unione, ferme restando le responsabilità formali degli altri livelli di dirigenza rispetto all'osservanza delle norme e alla gestione dei rischi di cibersicurezza nei rispettivi settori di competenza;

6) "quasi incidente": un quasi incidente quale definito all'articolo 6, punto 5), della direttiva (UE) 2022/2555;

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

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

10) "gestione degli incidenti": la gestione degli incidenti quale definita all'articolo 6, punto 8), della direttiva (UE) 2022/2555;

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

12) "minaccia informatica significativa": una minaccia informatica significativa quale definita all'articolo 6, punto 11), della direttiva (UE) 2022/2555;

13) "vulnerabilità": una vulnerabilità quale definita all'articolo 6, punto 15), della direttiva (UE) 2022/2555;

14) "rischio per la cibersicurezza": un rischio quale definito all'articolo 6, punto 9), della direttiva (UE) 2022/2555;

15) "servizio di cloud computing": un servizio di cloud computing quale definito all'articolo 6, punto 30), della direttiva (UE) 2022/2555.

Articolo 4

Trattamento dei dati personali

1. Il trattamento dei dati personali a norma del presente regolamento da parte del CERT-UE, del comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10 e dei soggetti dell'Unione è effettuato in conformità del regolamento (UE) 2018/1725.

2. Nello svolgimento dei compiti o nell'adempimento degli obblighi previsti dal presente regolamento, il CERT-UE, il comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10 e i soggetti dell'Unione trattano e scambiano i dati personali solo nella misura necessaria e al solo scopo di svolgere tali compiti o adempiere a tali obblighi.

3. Il trattamento di categorie particolari di dati personali di cui all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 è considerato necessario per motivi di interesse pubblico rilevante a norma dell'articolo 10, paragrafo 2, lettera g), di tale regolamento. Tali dati possono essere trattati solo nella misura necessaria per l'attuazione delle misure di gestione dei rischi per la cibersicurezza di cui agli articoli 6 e 8, per la fornitura di servizi da parte del CERT-UE a norma dell'articolo 13, per la condivisione di informazioni specifiche su un incidente a norma dell'articolo 17, paragrafo 3, e dell'articolo 18, paragrafo 3, per la condivisione di informazioni a norma dell'articolo 20, per gli obblighi di segnalazione a norma dell'articolo 21, per il coordinamento della risposta e la cooperazione in caso di incidenti a norma dell'articolo 22 e per la gestione degli incidenti gravi a norma dell'articolo 23 del presente regolamento. I soggetti dell'Unione e il CERT-UE, quando agiscono in qualità di titolari del trattamento, applicano misure tecniche per prevenire il trattamento di categorie particolari di dati personali per scopi diversi e prevedono misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati.

Capo II

Misure per un livello comune elevato di cibersicurezza

Articolo 5

Attuazione delle misure

1. Entro ... [otto mesi dalla data di entrata in vigore del presente regolamento], il comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10, previa consultazione dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e dopo aver ricevuto orientamenti dal CERT-UE, emana indirizzi destinati ai soggetti dell'Unione per effettuare un riesame iniziale della cibersicurezza e istituire un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza a norma dell'articolo 6, svolgere valutazioni di maturità della cibersicurezza a norma dell'articolo 7, adottare misure di gestione dei rischi per la cibersicurezza a norma dell'articolo 8 e adottare il piano di cibersicurezza a norma dell'articolo 9.

2. Nell'attuazione degli articoli da 6 a 9, i soggetti dell'Unione tengono conto degli indirizzi di cui al paragrafo 1 del presente articolo, nonché degli indirizzi e delle raccomandazioni pertinenti adottati a norma degli articoli 11 e 14.

Articolo 6

Quadro di gestione, di governance e di controllo dei rischi

1. Entro ... [15 mesi dalla data di entrata in vigore del presente regolamento], ogni soggetto dell'Unione, dopo aver effettuato un riesame iniziale della cibersicurezza, come un audit, istituisce un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza ("quadro"). L'istituzione del quadro è soggetta alla vigilanza del livello di dirigenza più elevato del soggetto dell'Unione ed è sotto la sua responsabilità.

2. Il quadro interessa la totalità dell'ambiente TIC non riservato del soggetto dell'Unione interessato, compresi ogni ambiente TIC e la rete di tecnologie operative in loco, le risorse e i servizi esternalizzati in ambienti di cloud computing od ospitati da terzi, i dispositivi mobili, le reti interne, le reti professionali non connesse a Internet e qualsiasi dispositivo connesso a tali ambienti ("ambiente TIC"). Il quadro è basato su un approccio multirischio.

3. Il quadro garantisce un livello elevato di cibersicurezza e stabilisce le politiche interne in materia di cibersicurezza, comprensive di obiettivi e priorità, per la sicurezza delle reti e dei sistemi informativi, nonché i ruoli e le responsabilità del personale del soggetto dell'Unione incaricato di garantire l'efficace attuazione del presente regolamento. Il quadro comprende anche meccanismi per misurare l'efficacia dell'attuazione.

4. Il quadro è riesaminato periodicamente in considerazione dell'evoluzione dei rischi per la cibersicurezza e almeno ogni quattro anni. Se del caso e a seguito di una richiesta del comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10, il quadro di un soggetto dell'Unione può essere aggiornato sulla base degli orientamenti del CERT-UE sugli incidenti identificati o sulle eventuali lacune osservate nell'attuazione del presente regolamento.

5. Il livello di dirigenza più elevato di ciascun soggetto dell'Unione è responsabile dell'attuazione del presente regolamento e vigila sul rispetto degli obblighi relativi al quadro da parte della propria organizzazione.

6. 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 obblighi specifici a norma del presente regolamento ad alti funzionari ai sensi dell'articolo 29, paragrafo 2, dello statuto dei funzionari o ad altri funzionari di livello equivalente, in seno al soggetto dell'Unione interessato. Indipendentemente da tale delega, il livello di gestione più elevato può essere ritenuto responsabile delle violazioni del presente regolamento da parte del soggetto dell'Unione interessato.

7. Ogni soggetto dell'Unione dispone di meccanismi efficaci per garantire che un'adeguata percentuale della dotazione di bilancio destinata alle TIC sia spesa per la cibersicurezza. Nel fissare tale percentuale è tenuto debitamente conto del quadro.

8. Ogni soggetto dell'Unione nomina un responsabile locale per la cibersicurezza o una funzione equivalente come 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 a cadenza periodica in merito allo stato di attuazione. Fermo restando che il responsabile locale per la cibersicurezza è il punto di contatto unico in ciascun soggetto dell'Unione, un soggetto dell'Unione può delegare determinati compiti del 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, oppure tali compiti possono essere condivisi tra vari soggetti dell'Unione. In caso di delega di tali compiti al CERT-UE, il comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10 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 il responsabile locale per la cibersicurezza nominato e le eventuali modifiche successive.

Il CERT-UE istituisce un elenco dei responsabili locali per la cibersicurezza nominati e lo mantiene aggiornato.

9. Gli alti funzionari di cui all'articolo 29, paragrafo 2, dello statuto dei funzionari o gli altri funzionari di livello equivalente di ciascun soggetto dell'Unione, così come tutti i membri pertinenti del personale incaricato dell'attuazione delle misure di gestione dei rischi per la cibersicurezza e dell'adempimento degli obblighi stabiliti dal presente regolamento, seguono periodicamente attività di formazione specifiche al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi per la cibersicurezza, le pratiche di gestione degli stessi e il loro impatto sulle attività del soggetto dell'Unione.

Articolo 7

Valutazioni di maturità della cibersicurezza

1. Entro ... [18 mesi dalla data di entrata in vigore del presente regolamento] e successivamente almeno ogni due anni, ciascun soggetto dell'Unione svolge una valutazione di maturità della cibersicurezza che comprende tutti gli elementi del proprio ambiente TIC.

2. Le valutazioni di maturità della cibersicurezza sono svolte, se del caso, con l'assistenza di terzi specializzati.

3. I soggetti dell'Unione con strutture simili possono cooperare nello svolgimento delle valutazioni di maturità della cibersicurezza per i rispettivi soggetti.

4. Sulla base di una richiesta del comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10 e con il consenso esplicito del soggetto dell'Unione interessato, i risultati di una valutazione di maturità della cibersicurezza possono essere discussi in seno a tale comitato o all'interno del gruppo informale di responsabili locali per la cibersicurezza al fine di trarre insegnamenti dalle esperienze e condividere le migliori pratiche.

Articolo 8

Misure di gestione dei rischi per la cibersicurezza

1. Senza indebito ritardo e comunque entro ... [20 mesi dalla data di entrata in vigore del presente regolamento], ogni soggetto dell'Unione adotta misure tecniche, operative e organizzative adeguate e proporzionate, sotto la vigilanza del livello di dirigenza più elevato, per gestire i rischi per la cibersicurezza individuati nell'ambito del quadro e per prevenire o ridurre al minimo l'impatto degli incidenti. Tenendo conto dello stato delle conoscenze e, se del caso, delle pertinenti norme europee e internazionali, tali misure garantiscono un livello di sicurezza dei sistemi informativi e di rete in tutto l'ambiente TIC commisurato ai rischi posti per la cibersicurezza. Nel valutare la proporzionalità di tali misure, è tenuto debitamente conto del grado di esposizione del soggetto dell'Unione ai rischi per la cibersicurezza, delle sue dimensioni, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale, economico e interistituzionale.

2. Nell'attuazione delle misure di gestione dei rischi per la cibersicurezza, i soggetti dell'Unione trattano almeno gli ambiti seguenti:

a) la politica in materia di cibersicurezza, comprese le misure necessarie per conseguire gli obiettivi e le priorità di cui all'articolo 6 e al paragrafo 3 del presente articolo;

b) le politiche di analisi dei rischi per la cibersicurezza e di sicurezza dei sistemi informativi;

c) gli obiettivi strategici relativi all'uso dei servizi di cloud computing;

d) un audit sulla cibersicurezza, se del caso, che può includere una valutazione dei rischi per la cibersicurezza, della vulnerabilità e delle minacce informatiche, e i test di penetrazione effettuati periodicamente da un fornitore privato affidabile;

e) l'attuazione delle raccomandazioni risultanti dagli audit sulla cibersicurezza di cui alla lettera d) mediante aggiornamenti delle politiche e della cibersicurezza;

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

g) la gestione delle risorse, compresi l'inventario delle risorse TIC e la cartografia della rete TIC;

h) la sicurezza delle risorse umane e il controllo degli accessi;

i) la sicurezza delle operazioni;

j) la sicurezza delle comunicazioni;

k) l'acquisizione, lo sviluppo e la manutenzione dei sistemi, comprese le politiche in materia di gestione e divulgazione delle vulnerabilità;

l) se possibile, le politiche in materia di trasparenza del codice sorgente;

m) la sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto dell'Unione e i suoi fornitori diretti o prestatori di servizi;

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

o) la gestione della continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e la gestione delle crisi; e

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

Ai fini del primo comma, lettera m), 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.

3. I soggetti dell'Unione adottano almeno le seguenti misure specifiche di gestione dei rischi per la cibersicurezza:

a) disposizioni tecniche per consentire e sostenere il telelavoro;

b) provvedimenti concreti per compiere progressi verso i principi fiducia zero;

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

d) l'uso della crittografia e della cifratura, in particolare della cifratura end-to-end, e della firma elettronica sicura;

e) se del caso, comunicazioni vocali, video e testuali sicure e sistemi di comunicazione di emergenza sicuri all'interno del soggetto dell'Unione;

f) misure proattive per l'identificazione e la rimozione di software maligni e spyware;

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

h) l'istituzione e l'adozione di programmi di formazione sulla cibersicurezza commisurati ai compiti prescritti e alle capacità attese, per il livello di dirigenza più elevato e per i membri del personale del soggetto dell'Unione incaricati di garantire l'efficace attuazione del presente regolamento;

i) la regolare formazione del personale in materia di cibersicurezza;

j) se del caso, la partecipazione nelle analisi dei rischi di interconnettività tra i soggetti dell'Unione;

k) 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 TIC e il CERT-UE;

   ii) gli obblighi contrattuali di segnalare gli incidenti, le vulnerabilità e le minacce informatiche, così come di avere predisposti adeguati meccanismi di risposta e controllo in caso di incidenti.

Articolo 9

Piani di cibersicurezza

1. A seguito della conclusione della valutazione di maturità della cibersicurezza svolta a norma dell'articolo 7 e considerando le risorse e i rischi per la cibersicurezza individuati nell'ambito del quadro e le misure di gestione dei rischi per la cibersicurezza adottate a norma dell'articolo 8, il livello di dirigenza più elevato di ogni soggetto dell'Unione approva, senza indebito ritardo e comunque entro... [24 mesi dalla data di entrata in vigore del presente regolamento], un piano di cibersicurezza. Il piano di cibersicurezza è volto ad aumentare la cibersicurezza complessiva del soggetto dell'Unione e contribuisce così al rafforzamento di un livello comune elevato di cibersicurezza all'interno dei soggetti dell'Unione. Il piano di cibersicurezza comprende come minimo le misure di gestione dei rischi per la cibersicurezza adottate in conformità dell'articolo 8. Il piano di cibersicurezza è rivisto ogni due anni o più spesso, se necessario, a seguito delle valutazioni di maturità della cibersicurezza svolte a norma dell'articolo 7 o di un riesame sostanziale del quadro.

2. Il piano di cibersicurezza comprende il piano di gestione delle crisi informatiche del soggetto dell'Unione per gli incidenti gravi.

3. Il soggetto dell'Unione trasmette il piano di cibersicurezza completo al comitato interistituzionale per la cibersicurezza istituito a norma dell'articolo 10.

Capo III

Comitato interistituzionale per la cibersicurezza

Articolo 10

Comitato interistituzionale per la cibersicurezza

1. È istituito un comitato interistituzionale per la cibersicurezza (IICB).

2. L'IICB ha il compito di:

   a) controllare e sostenere 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 e 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;

v) la Corte di giustizia dell'Unione europea;

vi) la Banca centrale europea;

vii) la Corte dei conti;

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 per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca;

xiii) l'ENISA;

xiv) il Garante europeo della protezione dei dati (GEPD);

xv) l'Agenzia dell'Unione europea per il programma spaziale;

b) tre rappresentanti designati dalla rete delle agenzie dell'Unione (EUAN) su proposta del suo comitato consultivo TIC per difendere gli interessi degli organi e degli organismi dell'Unione che gestiscono il proprio ambiente TIC diversi da quelli di cui alla lettera a).

I soggetti dell'Unione rappresentati nell'IICB mirano a conseguire l'equilibrio di genere tra i rappresentanti designati.

4. I membri dell'IICB possono farsi assistere da un supplente. Altri rappresentanti dei soggetti dell'Unione di cui al paragrafo 3 o di altri soggetti dell'Unione possono essere invitati dal presidente ad assistere alle riunioni dell'IICB senza avere diritto di voto.

5. Il direttore del CERT-UE e i presidenti del gruppo di cooperazione, della rete di CSIRT e della rete EU-CyCLONe, istituiti, rispettivamente, a norma degli articoli 14, 15 e 16 della direttiva (UE) 2022/2555, o i loro supplenti possono partecipare alle riunioni dell'IICB in qualità di osservatori. In casi eccezionali l'IICB può decidere diversamente, conformemente al proprio regolamento interno.

6. L'IICB adotta il proprio regolamento interno.

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

8. L'IICB si riunisce almeno tre volte all'anno su iniziativa del presidente, su richiesta del CERT-UE o su richiesta di uno dei membri.

9. Ciascun membro dell'IICB dispone di un voto. Le decisioni dell'IICB sono adottate a maggioranza semplice, salvo ove il presente regolamento disponga diversamente. Il presidente dell'IICB non dispone di un voto, tranne in caso di parità di voti, nel qual caso può esprimere il voto decisivo.

10. 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.

11. Le funzioni di segretariato dell'IICB sono espletate dalla Commissione e il segretariato rende conto al presidente dell'IICB.

12. I rappresentanti nominati dall'EUAN trasmettono le decisioni dell'IICB ai membri dell'EUAN. Ogni membro dell'EUAN ha la facoltà di sottoporre a tali rappresentanti 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. L'IICB stabilisce il regolamento interno del comitato esecutivo, compresi i suoi compiti e i suoi poteri, e il mandato dei suoi membri.

14. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento] e successivamente a cadenza annuale, l'IICB presenta al Parlamento europeo e 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 degli Stati membri in ciascuno Stato membro. La relazione costituisce un contributo alla relazione biennale sullo stato della cibersicurezza nell'Unione adottata a norma dell'articolo 18 della direttiva (UE) 2022/2555.

Articolo 11

Compiti dell'IICB

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

a) fornisce orientamenti al direttore del CERT-UE;

b) controlla e vigila efficacemente sull'attuazione del presente regolamento e sostiene i soggetti dell'Unione nel rafforzamento della loro cibersicurezza, anche, se del caso, richiedendo relazioni ad hoc ai soggetti dell'Unione e al CERT-UE;

c) previa discussione strategica, adotta una strategia pluriennale per innalzare il livello di cibersicurezza nei soggetti dell'Unione, valuta tale strategia periodicamente e comunque ogni cinque anni e, ove necessario, la modifica;

d) stabilisce la metodologia e gli aspetti organizzativi per lo svolgimento di riesami inter pares volontari da parte di soggetti dell'Unione, al fine di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità di cibersicurezza dei soggetti dell'Unione, garantendo che tali riesami inter pares siano condotti da esperti di cibersicurezza designati da un soggetto dell'Unione diverso da quello sottoposto al riesame e che la metodologia si basi sull'articolo 19 della direttiva (UE) 2022/2555 e sia, se del caso, adattata ai soggetti dell'Unione;

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

f) approva, sulla base di una proposta del direttore del CERT-UE, il catalogo dei servizi offerti dal CERT-UE e ogni suo aggiornamento;

g) approva, sulla base di una proposta del direttore del CERT-UE, la pianificazione finanziaria annuale delle entrate e delle spese, anche in materia di personale, per le attività del CERT-UE;

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

i) 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;

j) approva e controlla gli indicatori essenziali di prestazione per il CERT-UE stabiliti sulla base di una proposta del direttore del CERT-UE;

k) approva gli accordi di cooperazione, gli accordi sul livello dei servizi o i contratti tra il CERT-UE e altri soggetti ai sensi dell'articolo 18;

l) adotta indirizzi e raccomandazioni sulla base di una proposta del CERT-UE conformemente all'articolo 14 e dà istruzione al CERT-UE di emanare, ritirare o modificare una proposta relativa a indirizzi o raccomandazioni, o un invito a intervenire;

m) istituisce gruppi di consulenza tecnica con compiti specifici per assistere l'IICB nel suo operato, approva il loro mandato e ne designa i rispettivi presidenti;

n) riceve e valuta i documenti e le relazioni presentati dai soggetti dell'Unione a norma del presente regolamento, come le valutazioni di maturità della cibersicurezza;

o) facilita l'istituzione di un gruppo informale di responsabili locali della cibersicurezza dei soggetti dell'Unione, con il sostegno dell'ENISA, allo scopo di scambiare migliori pratiche e informazioni in relazione all'attuazione del presente regolamento;

p) tenendo conto delle informazioni sui rischi di cibersicurezza individuati e degli insegnamenti tratti dal CERT-UE, controlla l'adeguatezza degli accordi di interconnettività tra gli ambienti TIC dei soggetti dell'Unione e fornisce consulenza su eventuali miglioramenti;

q) istituisce un piano di gestione delle crisi informatiche al fine di sostenere, a livello operativo, la gestione coordinata degli incidenti gravi che colpiscono i soggetti dell'Unione e al fine di contribuire allo scambio regolare di informazioni pertinenti, in particolare per quanto riguarda l'impatto e l'entità degli incidenti gravi e i possibili modi per attenuarne gli effetti;

r) coordina l'adozione dei piani individuali di gestione delle crisi informatiche dei soggetti dell'Unione di cui all'articolo 9, paragrafo 2;

s) adotta raccomandazioni relative alla sicurezza delle catene di approvvigionamento di cui all'articolo 8, paragrafo 2, primo comma, lettera m), tenendo conto dei risultati delle valutazioni coordinate a livello dell'Unione dei rischi di sicurezza delle catene di approvvigionamento critiche di cui all'articolo 22 della direttiva (UE) 2022/2555 per sostenere i soggetti dell'Unione nell'adozione di misure di gestione dei rischi di cibersicurezza efficaci e proporzionate.

Articolo 12

Osservanza delle disposizioni

1. L'IICB, a norma dell'articolo 10, paragrafo 2, e dell'articolo 11, controlla efficacemente che i soggetti dell'Unione attuino il presente regolamento e gli indirizzi, le raccomandazioni e gli inviti a intervenire da loro adottati. L'IICB può chiedere ai soggetti dell'Unione le informazioni o la documentazione necessarie a tal fine. Ai fini dell'adozione di misure di osservanza ai sensi del presente articolo, il soggetto dell'Unione interessato, se è direttamente rappresentato nell'IICB, 'non ha diritto di voto.

2. Qualora constati che un soggetto dell'Unione non ha attuato efficacemente il presente regolamento o gli indirizzi, le raccomandazioni o gli inviti a intervenire emanati in base ad esso, ferme restando le procedure interne del soggetto dell'Unione interessato e dopo aver dato a quest'ultimo l'opportunità di presentare le proprie opinioni, l'IICB può:

   a) comunicare al soggetto dell'Unione interessato un parere motivato sulle carenze osservate nell'attuazione del presente regolamento;

   b) previa consultazione del CERT-UE, fornire indirizzi al soggetto dell'Unione interessato affinché il suo quadro, le sue misure di gestione del rischio di cibersicurezza, il suo piano di cibersicurezza e le sue relazioni si conformino al presente regolamento entro un termine specificato;

c) emanare un avvertimento per rimediare alle carenze individuate entro un termine specificato, comprese raccomandazioni per modificare le misure adottate dal soggetto dell'Unione interessato ai sensi del presente regolamento;

d) inviare una notifica motivata al soggetto dell'Unione interessato nel caso in cui entro il termine specificato non sia stato posto sufficiente rimedio alle carenze individuate in un avvertimento emanato a norma della lettera c);

e) emanare:

   i) una raccomandazione per l'esecuzione di un audit; o

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

f) se del caso, informare la Corte dei conti, nell'ambito del suo mandato, della presunta inosservanza;

g) emanare una raccomandazione affinché tutti gli Stati membri e i soggetti dell'Unione attuino una sospensione temporanea dei flussi di dati verso il soggetto dell'Unione interessato.

Ai fini del primo comma, lettera c), i destinatari dell'avvertimento sono adeguatamente circoscritti, se necessario in considerazione di un rischio per la cibersicurezza.

Gli avvertimenti e le raccomandazioni emanati ai sensi del primo comma sono indirizzati al livello di dirigenza più elevato del soggetto dell'Unione interessato.

3. Qualora l'IICB abbia adottato misure a norma del paragrafo 2, primo comma, lettere da a) a g), il soggetto dell'Unione interessato fornisce dettagli delle misure e azioni adottate per ovviare alle presunte carenze individuate dall'IICB. Il soggetto dell'Unione presenta tali dettagli entro un periodo di tempo ragionevole da concordare con l'IICB.

4. Qualora l'IICB ritenga che vi sia una violazione persistente 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 dell'Unione interessato di adottare misure appropriate, anche chiedendo di prendere in considerazione l'adozione di misure di natura disciplinare, conformemente alle norme e alle procedure stabilite nello statuto del personale e a qualsiasi altra norma e procedura applicabile. A tal fine, l'IICB trasferisce le informazioni necessarie al soggetto dell'Unione interessato.

5. Qualora i soggetti dell'Unione comunichino di non essere in grado di rispettare le scadenze di cui all'articolo 6, paragrafo 1, e all'articolo 8, paragrafo 1, l'IICB può, in casi debitamente motivati e tenendo conto delle dimensioni del soggetto dell'Unione, autorizzarne la proroga.

Capo IV
CERT-UE

Articolo 13

Missione e compiti del CERT-UE

1. La missione del CERT-UE consiste nel contribuire alla sicurezza dell'ambiente TIC non riservato dei soggetti dell'Unione fornendo loro consulenza in materia di cibersicurezza, aiutandoli a prevenire, rilevare, affrontare e attenuare gli incidenti e a rispondervi e riprendersi dagli stessi, e fungendo per tali soggetti da piattaforma per lo scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti.

2. Il CERT-UE raccoglie, gestisce, analizza e condivide informazioni con i soggetti dell'Unione sulle minacce informatiche, 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.

3. Il CERT-UE svolge i seguenti compiti per assistere i soggetti dell'Unione:

   a) li assiste nell'attuazione del presente regolamento e contribuisce al coordinamento della sua attuazione tramite le misure elencate all'articolo 14, paragrafo 1, o tramite relazioni ad hoc richieste dall'IICB;

b) offre servizi CSIRT standard per 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 17 e 18;

d) richiama l'attenzione dell'IICB su ogni problema relativo all'attuazione del presente regolamento e all'attuazione degli indirizzi, delle raccomandazioni e degli inviti a intervenire;

e) sulla base delle informazioni di cui al paragrafo 2, contribuisce alla consapevolezza situazionale informatica dell'Unione in stretta cooperazione con l'ENISA;

f) coordina la gestione degli incidenti gravi;

g) funge, per i soggetti dell'Unione, da equivalente del coordinatore designato ai fini della divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555;

h) fornisce, su richiesta di un soggetto dell'Unione, la scansione proattiva e non invasiva dei sistemi informativi e di rete accessibili al pubblico di tale soggetto dell'Unione.

Le informazioni di cui al primo comma, lettera e), sono condivise con l'IICB, la rete CSIRT e il Centro UE di situazione e di intelligence (INTCEN), ove applicabile e appropriato, e sono soggette ad adeguate condizioni di riservatezza.

4. Il CERT-UE può cooperare, conformemente all'articolo 17 o 18, a seconda dei casi, con le pertinenti comunità di cibersicurezza all'interno dell'Unione e dei suoi Stati membri, anche nei settori seguenti:

   a) preparazione, coordinamento in caso di incidente, scambio di informazioni e risposta alle crisi a livello tecnico relativamente a casi collegati ai soggetti dell'Unione;

   b) cooperazione operativa per quanto riguarda la rete CSIRT, anche per l'assistenza reciproca;

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

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

5. Nell'ambito 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. Il CERT-UE può cooperare e scambiare informazioni con il Centro per la lotta alla criminalità informatica di Europol.

6. 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 TIC dei soggetti dell'Unione, diversi da quelli di cui al paragrafo 3, forniti in base ad accordi sul livello dei servizi e compatibilmente con le risorse disponibili, in particolare il controllo della rete ad ampio spettro, compreso il controllo di prima linea 24 ore al giorno, 7 giorni su 7, per le minacce informatiche di gravità elevata;

b) servizi a sostegno di operazioni o progetti di cibersicurezza dei soggetti dell'Unione, diversi da quelli volti a proteggere il loro ambiente TIC, forniti in base ad accordi scritti e previa approvazione dell'IICB;

c) su richiesta, una scansione proattiva dei sistemi informativi e di rete del soggetto dell'Unione interessato per individuare le vulnerabilità con un potenziale impatto significativo;

d) servizi a sostegno della sicurezza dell'ambiente TIC di organizzazioni diverse dai 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.

Per quanto riguarda il primo comma, lettera d), in via eccezionale il CERT-UE può stipulare accordi sul livello dei servizi con soggetti diversi da quelli dell'Unione, previa approvazione dell'IICB.

7. Il CERT-UE organizza esercitazioni di cibersicurezza e può parteciparvi o raccomandare la partecipazione alle esercitazioni esistenti, se del caso in stretta cooperazione con l'ENISA, per verificare il livello di cibersicurezza dei soggetti dell'Unione.

8. Il CERT-UE può fornire assistenza ai soggetti dell'Unione in caso di incidenti in reti e sistemi informativi che trattano ICUE se i soggetti dell'Unione interessati lo richiedono esplicitamente in conformità delle rispettive procedure. La fornitura di assistenza da parte del CERT-UE ai sensi del presente paragrafo non pregiudica le norme applicabili in materia di protezione delle informazioni classificate.

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

10. Il CERT-UE fornisce, con un elevato livello di riservatezza e affidabilità, attraverso meccanismi di cooperazione e linee gerarchiche appropriati, informazioni pertinenti e anonimizzate sugli incidenti gravi e sul modo in cui sono stati gestiti. Tali informazioni sono inserite nella relazione di cui all’articolo 10, paragrafo 14.

11. Il CERT-UE, in collaborazione con il GEPD, sostiene i soggetti dell'Unione interessati nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti del GEPD in quanto autorità di controllo ai sensi del regolamento (UE) 2018/1725.

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

Articolo 14

Indirizzi, 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;

b) proposte all'IICB per indirizzi destinati a tutti i soggetti dell'Unione o a una parte di essi;

c) proposte all'IICB per raccomandazioni destinate a singoli soggetti dell'Unione.

Per quanto riguarda il primo comma, lettera a), il soggetto dell'Unione interessato, senza indebito ritardo dopo aver ricevuto l'invito a intervenire, informa il CERT-UE su come ha applicato le misure di sicurezza urgenti.

2. Gli indirizzi e le raccomandazioni possono contenere:

a) metodologie comuni e un modello per valutare la maturità della cibersicurezza dei soggetti dell'Unione, comprese le scale o gli indicatori essenziali di prestazione corrispondenti, destinati a servire da riferimento a sostegno del miglioramento continuo della cibersicurezza in tutti i soggetti dell'Unione e a facilitare l'assegnazione di priorità ai settori e alle misure di cibersicurezza tenendo conto della posizione di cibersicurezza dei soggetti;

b) modalità o miglioramenti riguardanti la gestione dei rischi per la cibersicurezza e le misure di gestione dei rischi di cibersicurezza;

c) modalità relative alle valutazioni di maturità della cibersicurezza e ai piani di cibersicurezza;

d) se del caso, disposizioni sull'utilizzo di una tecnologia, architettura, pratiche open source e relative migliori pratiche comuni allo scopo di conseguire interoperabilità e norme comuni, compreso un approccio coordinato alla sicurezza della catena di approvvigionamento;

e) se del caso, informazioni per agevolare l'uso di strumenti per appalti comuni volti all'acquisto presso fornitori terzi di pertinenti servizi e prodotti di cibersicurezza;

f) accordi di condivisione delle informazioni a norma dell'articolo 20.

Articolo 15

Direttore del CERT-UE

1. Dopo aver ottenuto l'approvazione da una maggioranza di due terzi dei membri dell'IICB, la Commissione nomina il direttore del CERT-UE. L'IICB è consultato in tutte le fasi della procedura di nomina, in particolare per quanto riguarda la redazione degli avvisi di posto vacante, l'esame delle candidature e la designazione delle commissioni giudicatrici in relazione a tale incarico. La procedura di selezione, compreso l'elenco ristretto definitivo di candidati tra i quali deve essere nominato il direttore del CERT-UE, garantisce un'equa rappresentanza di ciascun genere, tenendo conto delle domande presentate.

2. Il direttore del CERT-UE è responsabile del buon funzionamento del CERT-UE e agisce nei limiti delle sue attribuzioni e sotto la direzione dell'IICB. Il direttore del CERT-UE riferisce regolarmente al presidente dell'IICB e presenta relazioni ad hoc all'IICB, se questo lo richiede.

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 74, paragrafo 9, del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio[1], e riferisce periodicamente all'ordinatore delegato 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, una proposta di programma di lavoro annuale, una proposta di catalogo dei servizi per il CERT-UE, proposte di revisione del catalogo dei servizi, proposte di modalità riguardanti gli accordi sul livello dei servizi e proposte di indicatori essenziali di prestazione per il CERT-UE, che devono essere approvate dall'IICB conformemente all'articolo 11. 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.

---

[1] 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).

5. Il direttore del CERT-UE presenta a cadenza almeno annuale all'IICB e al presidente dell'IICB relazioni riguardanti le attività e le prestazioni del CERT-UE durante il periodo di riferimento, inclusi 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 11. Tali relazioni comprendono un programma di lavoro per il periodo successivo, la pianificazione finanziaria delle entrate e delle spese, anche relative al personale, gli aggiornamenti previsti del catalogo dei servizi offerti dal CERT-UE e una valutazione dell'impatto previsto di tali aggiornamenti relativamente alle risorse finanziarie e umane.

Articolo 16

Questioni finanziarie e relative al personale

1. Il CERT-UE è integrato nella struttura amministrativa di una direzione generale della Commissione al fine di beneficiare delle strutture di sostegno amministrativo, finanziario e contabile della Commissione, mantenendo nel contempo il suo status di prestatore di servizi interistituzionale autonomo per tutti i soggetti dell'Unione. La Commissione informa l'IICB in merito alla collocazione amministrativa del CERT-UE e a eventuali cambiamenti al riguardo. La Commissione riesamina le disposizioni amministrative relative al CERT-UE periodicamente e in ogni caso prima della definizione di un quadro finanziario pluriennale a norma dell'articolo 312 TFUE, al fine di consentire l'adozione di misure adeguate. Il riesame include la possibilità di istituire il CERT-UE come organismo dell'Unione.

2. Per l'applicazione delle procedure amministrative e finanziarie, il direttore del CERT-UE agisce sotto l'autorità della Commissione e sotto la supervisione dell'IICB.

3. I compiti e le attività del CERT-UE, compresi i servizi da esso prestati ai sensi dell'articolo 13, paragrafi 3, 4, 5 e 7, e dell'articolo 14, 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 del presente articolo forniscono un contributo finanziario annuale al CERT-UE per coprire i servizi da esso prestati ai sensi dello stesso paragrafo. I contributi sono basati su orientamenti dati dall'IICB e concordati tra ciascun soggetto dell'Unione 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 del presente articolo, come entrate con destinazione specifica interna ai sensi dell'articolo 21, paragrafo 3, lettera c), del regolamento (UE, Euratom) 2018/1046.

5. I costi dei servizi di cui all'articolo 13, paragrafo 6, 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.

Articolo 17

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

1. Il CERT-UE coopera e scambia informazioni con omologhi degli Stati membri senza indebito ritardo, in particolare con gli CSIRT designati o istituiti a norma dell'articolo 10 della direttiva (UE) 2022/2555 o, se del caso, con le autorità competenti e i punti di contatto unici designati o istituiti a norma dell'articolo 8 di tale direttiva, riguardo a incidenti, minacce informatiche, vulnerabilità, quasi incidenti, possibili contromisure e migliori pratiche e su tutte le questioni pertinenti per migliorare la protezione degli ambienti TIC dei soggetti dell'Unione, anche mediante la rete CSIRT istituita a norma dell'articolo 15 della direttiva (UE) 2022/2555. Il CERT-UE sostiene la Commissione in seno all'EU-CyCLONe istituito a norma dell'articolo 16 della direttiva (UE) 2022/2555 in merito alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala.

2. Quando viene a conoscenza di un incidente significativo che si verifica nel territorio di uno Stato membro, il CERT-UE informa senza indugio gli omologhi pertinenti di quello Stato membro, in conformità del paragrafo 1.

3. A condizione che i dati personali siano protetti conformemente al diritto dell'Unione applicabile in materia di protezione dei dati, il CERT-UE scambia senza indebito ritardo informazioni pertinenti specifiche su un incidente con gli omologhi degli Stati membri per facilitare il rilevamento di minacce informatiche o incidenti analoghi o per contribuire all'analisi di un incidente, senza l'autorizzazione del soggetto dell'Unione interessato. Il CERT-UE scambia informazioni specifiche su un incidente che rivelino l'identità del bersaglio dell'incidente di cibersicurezza solo in uno dei casi seguenti:

a) il soggetto dell'Unione interessato vi acconsente;

b) il soggetto dell'Unione interessato non vi acconsente come stabilito alla lettera a), ma la diffusione dell'identità del soggetto dell'Unione interessato aumenterebbe la probabilità di evitare o attenuare incidenti altrove;

c) il soggetto dell'Unione interessato ha già reso pubblico il proprio coinvolgimento.

Le decisioni di scambiare informazioni specifiche su un incidente che rivelino l'identità del bersaglio a norma del primo comma, lettera b), sono avallate dal direttore del CERT-UE. Prima di emettere tale decisione, il CERT-UE contatta per iscritto il soggetto dell'Unione interessato, spiegando chiaramente in che modo la divulgazione della sua identità contribuirebbe a evitare o attenuare incidenti altrove. Il direttore del CERT-UE fornisce la spiegazione e chiede esplicitamente al soggetto dell'Unione di dichiarare se acconsente entro un termine stabilito. Il direttore del CERT-UE informa inoltre il soggetto dell'Unione che, alla luce della spiegazione fornita, si riserva il diritto di divulgare le informazioni anche in assenza di consenso. Il soggetto dell'Unione interessato è informato prima che le informazioni siano divulgate.

Articolo 18

Cooperazione tra il CERT-UE ed altri omologhi

1. Il CERT-UE può cooperare con omologhi nell'Unione diversi da quelli di cui all'articolo 17 che siano soggetti ai requisiti dell'Unione in materia di cibersicurezza, 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. Se il CERT-UE istituisce una cooperazione con tali omologhi, ne informa gli omologhi degli Stati membri pertinenti di cui all'articolo 17, paragrafo 1, nello Stato membro in cui è situato l'omologo. Ove applicabile e opportuno, tale cooperazione e le relative condizioni, anche per quanto riguarda la cibersicurezza, la protezione dei dati e il trattamento delle informazioni, sono stabilite in specifici accordi di riservatezza, quali contratti o accordi amministrativi.

   Gli accordi di riservatezza non sono subordinati all'approvazione preventiva dell'IICB, ma il suo presidente ne è informato. In caso di necessità urgente e imminente di scambiare informazioni sulla cibersicurezza nell'interesse dei soggetti dell'Unione o di un'altra parte, il CERT-UE può farlo con un soggetto le cui competenze, capacità e conoscenze specifiche sono legittimamente necessarie per rispondere a tale necessità urgente e imminente, anche se il CERT-UE non dispone di un accordo di riservatezza con tale soggetto. In tali casi il CERT-UE informa immediatamente il presidente dell'IICB e riferisce all'IICB mediante relazioni o riunioni periodiche.

2. Il CERT-UE può cooperare con partner, quali i soggetti commerciali, compresi i soggetti di settori specifici, le organizzazioni internazionali, gli enti nazionali non dell'Unione o i singoli esperti, al fine di raccogliere informazioni su minacce informatiche generali e specifiche, quasi incidenti, vulnerabilità e 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. Con il consenso del soggetto dell'Unione interessato da un incidente e a condizione che esista un accordo o un contratto di non divulgazione con l'omologo o il partner interessato, il CERT-UE può fornire informazioni in merito all'incidente specifico agli omologhi o ai partner di cui ai paragrafi 1 e 2 unicamente al fine di contribuire alla sua analisi.

Capo V
Cooperazione e obblighi di segnalazione

Articolo 19
Trattamento delle informazioni

1. I soggetti dell'Unione e il CERT-UE rispettano l'obbligo del segreto professionale ai sensi dell'articolo 339 TFUE o di equivalenti quadri normativi applicabili.

2. Alle richieste di accesso del pubblico ai documenti detenuti dal CERT-UE si applica il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[1], compreso l'obbligo, previsto da tale regolamento, di consultare altri soggetti dell'Unione o, se del caso, altri Stati membri, qualora la domanda riguardi loro documenti.

3. Il trattamento delle informazioni da parte dei soggetti dell'Unione e del CERT-UE si conforma alle norme applicabili sulla sicurezza delle informazioni.

Articolo 20

Accordi di condivisione delle informazioni sulla cibersicurezza

1. Su base volontaria, i soggetti dell'Unione possono notificare e fornire informazioni al CERT-UE sugli incidenti, le minacce informatiche, i quasi incidenti e le vulnerabilità che li interessano. Il CERT-UE garantisce la disponibilità di mezzi di comunicazione efficaci, con un livello elevato di tracciabilità, riservatezza e affidabilità, per agevolare la condivisione delle informazioni con i soggetti dell'Unione. Nel trattare le notifiche, il CERT-UE può dare la priorità al trattamento delle notifiche obbligatorie rispetto alle notifiche volontarie. Fatto salvo l'articolo 12, la notifica volontaria non deve avere l'effetto di imporre al soggetto dell'Unione che la effettua alcun obbligo aggiuntivo cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

---

1 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).

2. Per svolgere la missione e i compiti conferitigli a norma dell'articolo 13, il CERT-UE può chiedere ai soggetti dell'Unione di fornirgli informazioni tratte dai loro rispettivi inventari dei sistemi TIC, comprese le 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. Il soggetto dell'Unione cui è rivolta tale domanda trasmette senza indebito ritardo le informazioni richieste e ogni loro successivo aggiornamento.

3. Il CERT-UE può scambiare con i soggetti dell'Unione informazioni specifiche su un incidente che rivelino l'identità del soggetto dell'Unione interessato dall'incidente, a condizione che quest'ultimo vi acconsenta. Ove rifiuti il consenso, il soggetto dell'Unione fornisce al CERT-UE i motivi a sostegno di tale decisione.

4. I soggetti dell'Unione condividono con il Parlamento europeo e il Consiglio, su richiesta, informazioni relative al completamento dei piani di cibersicurezza.

5. L'IICB o il CERT-UE, a seconda dei casi, condividono con il Parlamento europeo e il Consiglio, su richiesta, indirizzi, raccomandazioni e inviti ad agire.

6. Gli obblighi di condivisione stabiliti nel presente articolo non comprendono:

   a) le ICUE;

b) le informazioni la cui ulteriore distribuzione è stata esclusa mediante un contrassegno visibile, a meno che la loro condivisione con il CERT-UE non sia stata esplicitamente consentita.

Articolo 21

Obblighi di segnalazione

1. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa per il funzionamento del soggetto dell'Unione interessato o perdite finanziarie per lo stesso;

b) ha interessato o è in grado di interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali.

2. 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 è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero o che interessi diversi soggetti;

b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica di incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva 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 della situazione;

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

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

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

   iii) le misure di attenuazione adottate e in corso;

   iv) se del caso, l'impatto transfrontaliero o su diversi soggetti dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

3. Un soggetto dell'Unione informa gli omologhi pertinenti degli Stati membri di cui all'articolo 17, paragrafo 1, nello Stato membro in cui ha sede del fatto che si è verificato un incidente significativo, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza.

4. I soggetti dell'Unione notificano, tra l'altro, eventuali informazioni che consentano al CERT-UE di determinare l'impatto su diversi soggetti, l'impatto sullo Stato membro ospitante o l'impatto transfrontaliero a seguito di un incidente significativo. Fatto salvo l'articolo 12, la sola notifica non espone il soggetto dell'Unione a una maggiore responsabilità.

5. Se del caso, i soggetti dell'Unione comunicano, senza indebito ritardo, agli utenti dei sistemi informativi e di rete interessati, o di altre componenti dell'ambiente TIC, che sono potenzialmente interessati da un incidente significativo o una minaccia informatica significativa e, se del caso, che devono adottare misure di attenuazione, qualsiasi misura o azione correttiva che possano adottare in risposta a tale incidente o minaccia. Se del caso, i soggetti dell'Unione informano tali utenti della minaccia informatica significativa stessa.

6. Qualora un incidente significativo o una minaccia informatica significativa interessi un sistema informativo e di rete o una componente dell'ambiente TIC di un soggetto dell'Unione intenzionalmente connesso con l'ambiente TIC di un altro soggetto dell'Unione, il CERT-UE emette una segnalazione di cibersicurezza.

7. I soggetti dell'Unione, su richiesta del CERT-UE, forniscono senza indebito ritardo al CERT-UE le informazioni digitali generate dall'uso dei dispositivi elettronici coinvolti nei loro rispettivi incidenti. Il CERT-UE può fornire ulteriori dettagli sui tipi di informazioni di cui ha bisogno ai fini della consapevolezza situazionale e della risposta agli incidenti.

8. Il CERT-UE trasmette ogni tre mesi all'IICB, all'ENISA, all'EU INTCEN e alla rete CSIRT una relazione di sintesi che comprende dati anonimizzati e aggregati su incidenti significativi, incidenti, minacce informatiche, quasi incidenti e vulnerabilità a norma dell'articolo 20 e sugli incidenti significativi notificati conformemente al paragrafo 2 del presente articolo. La relazione di sintesi costituisce un contributo alla relazione biennale sullo stato della cibersicurezza nell'Unione adottata a norma dell'articolo 18 della direttiva (UE) 2022/2555.

9. Entro ... [sei mesi dalla data di entrata in vigore del presente regolamento], l'IICB emana indirizzi o raccomandazioni che precisano ulteriormente le modalità, il formato e il contenuto della segnalazione a norma del presente articolo. Nell'elaborare tali indirizzi o raccomandazioni, l'IICB tiene conto degli atti di esecuzione adottati a norma dell'articolo 23, paragrafo 11, della direttiva (UE) 2022/2555, che specificano il tipo di informazioni, il formato e la procedura di notifica. Il CERT-UE diffonde gli adeguati dettagli tecnici che consentano l'adozione di misure proattive di rilevamento, risposta agli incidenti o attenuazione da parte dei soggetti dell'Unione.

10. Gli obblighi di segnalazione stabiliti nel presente articolo non comprendono:

a) le ICUE;

b) le informazioni la cui ulteriore distribuzione è stata esclusa mediante un contrassegno visibile, a meno che la loro condivisione con il CERT-UE non sia stata esplicitamente consentita.

Articolo 22

Coordinamento della risposta in caso di incidenti e cooperazione

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

a) i soggetti dell'Unione;

b) gli omologhi di cui agli articoli 17 e 18.

2. Il CERT-UE, se del caso in stretta cooperazione con l'ENISA, facilita il coordinamento fra i soggetti dell'Unione in materia di risposta agli incidenti, anche tramite:

a) il contributo a una comunicazione esterna coerente;

b) il sostegno reciproco, come la condivisione di informazioni pertinenti per i soggetti dell'Unione o la fornitura di assistenza, se del caso direttamente in loco;

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 degli incidenti, delle minacce informatiche, delle vulnerabilità e dei quasi incidenti, nonché la condivisione dei pertinenti sviluppi nel settore della cibersicurezza.

4. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento], l'IICB, sulla base di una proposta del CERT-UE, adotta indirizzi o raccomandazioni sul coordinamento della risposta in caso di incidenti e sulla cooperazione in caso di incidenti significativi. In caso di sospetta natura penale di un incidente, il CERT-UE fornisce consulenza su come segnalare l'incidente alle autorità di contrasto senza indebito ritardo.

5. A seguito di una richiesta specifica di uno Stato membro e con l'approvazione dei soggetti dell'Unione interessati, il CERT-UE può rivolgersi a esperti dell'elenco di cui all'articolo 23, paragrafo 4, per contribuire alla risposta a un incidente grave che ha un impatto in tale Stato membro o a un incidente di cibersicurezza su vasta scala conformemente all'articolo 15, paragrafo 3, lettera g), della direttiva (UE) 2022/2555. Le norme specifiche sull'accesso e il ricorso agli esperti tecnici dei soggetti dell'Unione sono approvate dall'IICB su proposta del CERT-UE.

Articolo 23

Gestione degli incidenti gravi

1. Al fine di sostenere a livello operativo la gestione coordinata degli incidenti gravi 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 istituisce, a norma dell'articolo 11, lettera q), un piano di gestione delle crisi informatiche basato sulle attività di cui all'articolo 22, paragrafo 2, in stretta cooperazione con il CERT-UE e l'ENISA. Il piano di gestione delle crisi informatiche comprende almeno gli elementi seguenti:

   a) disposizioni relative al coordinamento e al 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.

2. Fatto salvo il piano di gestione delle crisi informatiche istituito a norma del paragrafo 1 del presente articolo e fatto salvo l'articolo 16, paragrafo 2, primo comma, della direttiva (UE) 2022/2555, il rappresentante della Commissione nell'IICB è il punto di contatto per la condivisione delle informazioni pertinenti in relazione agli incidenti gravi con EU-CyCLONe.

3. Il CERT-UE coordina, fra i soggetti dell'Unione, la gestione degli incidenti gravi. Tiene un inventario delle competenze tecniche disponibili che risulterebbero necessarie per la risposta agli incidenti in caso di incidenti gravi e assiste l'IICB nel coordinare i piani di gestione delle crisi informatiche dei soggetti dell'Unione per gli incidenti gravi di cui all'articolo 9, paragrafo 2.

4. 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.

Capo VI
Disposizioni finali

Articolo 24

Riassegnazione di bilancio iniziale

Al fine di garantire il corretto e stabile funzionamento del CERT-UE, la Commissione può proporre la riassegnazione di personale e risorse finanziarie al proprio bilancio da utilizzare nelle operazioni del CERT-UE. La riassegnazione è effettiva contestualmente al primo bilancio annuale dell'Unione adottato dopo l'entrata in vigore del presente regolamento.

Articolo 25

Riesame

1. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento] e successivamente con frequenza annuale, l'IICB, coadiuvato dal CERT-UE, riferisce alla Commissione in merito all'attuazione del presente regolamento. L'IICB può rivolgere raccomandazioni alla Commissione per il riesame del presente regolamento.

2. Entro ... [36 mesi dalla data di entrata in vigore del presente regolamento] e successivamente ogni due anni, la Commissione valuta e riferisce al Parlamento europeo e al Consiglio in merito all'attuazione del presente regolamento e all'esperienza acquisita a livello strategico e operativo.

La relazione di cui al primo comma del presente paragrafo include il riesame di cui all'articolo 16, paragrafo 1, sulla possibilità di istituire il CERT-UE come ufficio dell'Unione.

3. Entro ... [cinque anni dalla data di entrata in vigore del presente regolamento], la Commissione valuta il funzionamento del presente regolamento e presenta una relazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. La Commissione valuta inoltre l'opportunità di includere nell'ambito di applicazione del presente regolamento le reti e i sistemi informativi che trattano ICUE, tenendo conto di altri atti legislativi dell'Unione applicabili a tali sistemi. La relazione, se necessario, è corredata di una proposta legislativa.

Articolo 26

Entrata in vigore

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

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

Fatto a Strasburgo,

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