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»)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di comunicazione elettronica svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione (TIC) sono alla base dei sistemi complessi su cui poggiano le attività quotidiane della società, fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, organizzazioni e imprese di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'Internet degli oggetti (*Internet of Things* — IoT) nel prossimo decennio dovrebbero essere disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. La rete e i sistemi informativi sono in grado di aiutarci in tutti gli aspetti della vita e danno impulso alla crescita economica dell'Unione. Sono fondamentali per il raggiungimento del mercato unico digitale.

(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi connessi alla cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), quali definite nella raccomandazione della Commissione 2003/361/CE ([4]), fino ai gestori delle infrastrutture critiche.

([1]) GU C 227 del 28.6.2018, pag. 86.
([2]) GU C 176 del 23.5.2018, pag. 29.
([3]) Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.
([4]) Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

(4) Mettendo a disposizione del pubblico le informazioni pertinenti, l'Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security* — ENISA), istituita dal regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio ([5]), contribuisce allo sviluppo del settore della cibersicurezza nell'Unione, in particolare le PMI e le start-up. L'ENISA dovrebbe puntare a una cooperazione più stretta con le università e gli istituti di ricerca al fine di contribuire alla riduzione della dipendenza da prodotti e servizi della cibersicurezza provenienti dall'esterno dell'Unione e a rinforzare le filiere all'interno dell'Unione.

(5) Gli attacchi informatici sono in aumento e la maggiore vulnerabilità alle minacce e agli attacchi informatici di un'economia e di una società connesse impone un rafforzamento delle difese. Tuttavia, mentre gli attacchi informatici avvengono spesso attraverso le frontiere, le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali. Gli incidenti su vasta scala possono ostacolare la prestazione di servizi essenziali in tutto il territorio dell'Unione. Ciò richiede capacità effettive e coordinate di risposta e di gestione delle crisi a livello di Unione, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca. Inoltre, una valutazione periodica dello stato della cibersicurezza e della resilienza nell'Unione, che sia basata su dati affidabili a livello di Unione, e previsioni sistematiche degli sviluppi, delle sfide e delle minacce futuri, a livello di Unione e a livello mondiale, sono importanti per i responsabili delle politiche, il settore e gli utenti.

(6) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura il rafforzamento ulteriore delle capacità e della preparazione degli Stati membri e delle imprese e il miglioramento della cooperazione, la condivisione di informazioni e il coordinamento tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare nei casi di crisi e incidenti transfrontalieri su vasta scala, pur tenendo conto dell'importanza di mantenere e rafforzare ulteriormente le capacità nazionali di risposta alle minacce informatiche di qualsiasi dimensione.

(7) Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la cibersicurezza. In aggiunta, dato che gli incidenti minano la fiducia nei fornitori di servizi digitali e nel mercato unico digitale stesso, soprattutto fra i consumatori, essa dovrebbe essere ulteriormente rafforzata fornendo informazioni in maniera trasparente in merito al livello di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC che evidenzi che persino un livello elevato di certificazione della cibersicurezza non può garantire che un prodotto TIC, un servizio TIC o un processo TIC sia completamente sicuro. Un aumento di fiducia può essere agevolato da una certificazione a livello di Unione che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

(8) La cibersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'«igiene informatica», vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche.

(9) Al fine di rafforzare le strutture della cibersicurezza dell'Unione, è importante mantenere e sviluppare le capacità degli Stati membri di rispondere in modo globale alle minacce informatiche, compresi gli incidenti transfrontalieri.

(10) Le imprese e i singoli consumatori dovrebbero disporre di informazioni precise sul livello di affidabilità con cui è stata certificata la sicurezza dei loro prodotti TIC, servizi TIC e processi TIC. Allo stesso tempo, nessun prodotto TIC o servizio TIC garantisce completamente la cibersicurezza e bisogna promuovere regole basilari sull'igiene informatica, dando loro la priorità. Alla luce della crescente disponibilità di dispositivi IoT, vi è una serie di misure volontarie che il settore privato può adottare per rafforzare la fiducia nella sicurezza dei prodotti TIC, servizi TIC e processi TIC.

(11) I moderni prodotti e sistemi TIC spesso integrano e utilizzano una o più tecnologie e componenti terzi quali moduli software, biblioteche o interfacce per programmi applicativi. Tale utilizzo, detto «dipendenza», potrebbe presentare rischi supplementari connessi alla cibersicurezza in quanto le vulnerabilità riscontrate in componenti terzi potrebbero pregiudicare anche la sicurezza dei prodotti TIC, servizi TIC e processi TIC. In molti casi, l'individuazione e la documentazione di tali dipendenze consentono agli utenti finali dei prodotti TIC, servizi TIC e processi TIC di migliorare le loro attività di gestione dei rischi in materia di cibersicurezza ottimizzando, ad esempio, le procedure messe in atto per individuare le vulnerabilità e porvi rimedio.

([5]) Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).

(12) Le organizzazioni, i fabbricanti o i fornitori coinvolti nella progettazione e nello sviluppo di prodotti TIC, servizi TIC e processi TIC dovrebbero essere incoraggiati ad attuare misure nelle prime fasi di progettazione e sviluppo per tutelare il più possibile sin dall'inizio la sicurezza di tali prodotti, servizi e processi, in modo che si presuma il verificarsi di attacchi informatici e se ne anticipi e riduca al minimo l'impatto («sicurezza fin dalla progettazione»). La sicurezza dovrebbe essere assicurata in tutto il ciclo di vita del prodotto TIC, servizio TIC o processo TIC, con un'evoluzione costante dei processi di progettazione e sviluppo al fine di ridurre il rischio di danni derivanti da un utilizzo doloso.

(13) Le imprese, le organizzazioni e il settore pubblico dovrebbero configurare i prodotti TIC, servizi TIC o processi TIC da loro progettati in modo da garantire un livello di sicurezza superiore che dovrebbe consentire al primo utente di ricevere una configurazione predefinita con le impostazioni più sicure possibili («sicurezza predefinita»), riducendo al contempo l'onere in capo agli utenti di dover configurare un prodotto TIC, servizio TIC o processo TIC in modo adeguato. La sicurezza predefinita non dovrebbe necessitare di configurazioni dettagliate né di conoscenze tecniche specifiche o di un comportamento non intuitivo da parte dell'utente, e dovrebbe funzionare in modo semplice e affidabile quando attuata. Qualora, su base puntuale, un'analisi del rischio e dell'usabilità porti a concludere che tali impostazioni predefinite non sono attuabili, gli utenti dovrebbero essere sollecitati a optare per l'impostazione più sicura.

(14) Il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio ([6]) ha istituito l'ENISA al fine di contribuire ad assicurare un livello di sicurezza elevato ed efficace delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni pubbliche. Il regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio ([7]) ha prorogato il mandato dell'ENISA fino a marzo 2012. Il regolamento (EU) n. 580/2011 del Parlamento europeo e del Consiglio ([8]) ha prorogato ulteriormente il mandato dell'ENISA fino al 13 settembre 2013. Il regolamento (UE) n. 526/2013 ha prorogato il mandato dell'ENISA fino al 19 giugno 2020.

(15) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la Strategia dell'Unione europea per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi informatici. Nell'intento di proteggere maggiormente i cittadini online, nel 2016 è stato adottato il primo atto giuridico nel campo della cibersicurezza, vale a dire la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([9]). La direttiva (UE) 2016/1148 ha stabilito obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, fornitura e distribuzione di acqua potabile, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di *cloud computing* e mercati online).

All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza. Altri atti giuridici, quali il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([10]) e le direttive 2002/58/CE ([11]) e (UE) 2018/1972 ([12]) del Parlamento europeo e del Consiglio, contribuiscono inoltre a un elevato livello di cibersicurezza nel mercato unico digitale.

([6]) Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1).

([7]) Regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008, pag. 1).

([8]) Regolamento (UE) n. 580/2011 del Parlamento europeo e del Consiglio, dell'8 giugno 2011, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 165 del 24.6.2011, pag. 3).

([9]) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

([10]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([11]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([12]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

(16) Dall'adozione della Strategia dell'Unione europea per la cibersicurezza nel 2013 e dall'ultima revisione del mandato dell'ENISA, il contesto politico generale è cambiato in modo significativo, in quanto il contesto globale è diventato più incerto e meno sicuro. Data la situazione e considerato lo sviluppo positivo del ruolo dell'ENISA quale punto di riferimento per pareri e competenze e facilitatore della cooperazione e dello sviluppo delle capacità, nonché nel quadro della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama della minaccia informatica, a fronte del quale l'attuale mandato non è sufficiente, come riconosciuto in fase di valutazione dell'ENISA.

(17) L'ENISA istituita dal presente regolamento dovrebbe succedere all'ENISA istituita con il regolamento (UE) n. 526/2013. L'ENISA dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli altri atti giuridici dell'Unione nel campo della cibersicurezza, anche fornendo pareri e competenze e fungendo da centro di informazioni e conoscenze dell'Unione. Dovrebbe promuovere lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornire suggerimenti strategici alla Commissione e agli Stati membri, fungere da punto di riferimento per iniziative politiche settoriali dell'Unione sulle questioni di cibersicurezza e promuovere la cooperazione operativa, sia tra gli Stati membri sia tra questi ultimi e le istituzioni, gli organi e gli organismi dell'Unione.

(18) Nel quadro della decisione 2004/97/CE, Euratom adottata di comune accordo dai rappresentanti dei governi degli Stati membri, riuniti a livello di capi di Stato o di governo ([13]), i rappresentanti degli Stati membri hanno deciso che la sede dell'ENISA sarebbe stata in Grecia, in una città designata dal governo greco. Lo Stato membro ospitante dovrebbe garantire le migliori condizioni possibili per il corretto ed efficace funzionamento dell'ENISA. Per uno svolgimento adeguato ed efficiente dei suoi compiti, per l'assunzione e il trattenimento del personale e per aumentare l'efficacia delle attività di rete, è imprescindibile che l'ENISA sia ubicata in una sede adeguata che garantisca, tra l'altro, collegamenti e infrastrutture di trasporto appropriati per i coniugi e i figli del personale. Le disposizioni necessarie dovrebbero essere fissate in un accordo concluso tra l'ENISA e lo Stato membro ospitante, previa approvazione del consiglio di amministrazione dell'ENISA.

(19) Tenuto conto dei rischi e delle sfide crescenti in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'ENISA dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale dell'Unione, consentendo all'ENISA di svolgere efficacemente i compiti che le sono conferiti dal presente regolamento.

(20) È opportuno che l'ENISA sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'ENISA dovrebbe sostenere attivamente gli sforzi nazionali e contribuire in modo proattivo agli sforzi dell'Unione, collaborando pienamente con le istituzioni, gli organi e gli organismi dell'Unione e con gli Stati membri, evitando la duplicazione delle attività e promuovendo le sinergie. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione del settore privato e di altri portatori d'interessi. È opportuno stabilire una serie di compiti che definiscano in che modo l'ENISA debba raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione.

(21) Per poter fornire adeguato sostegno alla cooperazione operativa tra gli Stati membri, l'ENISA dovrebbe rafforzare ulteriormente le proprie capacità e abilità tecniche e umane. L'ENISA dovrebbe incrementare il proprio know-how e le proprie capacità. L'ENISA e gli Stati membri, su base volontaria, potrebbero sviluppare programmi per il distacco di esperti nazionali presso l'ENISA, la creazione di pool di esperti e lo scambio di personale.

(22) L'ENISA dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione, l'aggiornamento e la revisione di politiche e normative nel campo della cibersicurezza, nonché i relativi aspetti settoriali al fine di rafforzare la pertinenza delle politiche e normative dell'Unione aventi una dimensione di cibersicurezza e assicurarne la coerenza dell'attuazione a livello nazionale. L'ENISA dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative settoriali dell'Unione che presentano aspetti correlati alla cibersicurezza. L'ENISA dovrebbe informare periodicamente il Parlamento europeo in merito alle sue attività.

([13]) Decisione 2004/97/CE, Euratom adottata di comune accordo dai rappresentanti dei governi degli Stati membri, riuniti a livello di capi di Stato o di governo, del 13 dicembre 2003, relativa alla fissazione delle sedi di taluni uffici ed agenzie dell'Unione europea (GU L 29 del 3.2.2004, pag. 15).

(23) Il nucleo pubblico dell'Internet aperta, vale a dire i suoi protocolli e le sue infrastrutture principali, che costituiscono un bene pubblico globale, consente la funzionalità essenziale di Internet nel suo complesso e ne supporta il normale funzionamento. L'ENISA dovrebbe sostenere la sicurezza del nucleo pubblico dell'Internet aperta e la stabilità del suo funzionamento, compresi, solo a titolo di esempio, i protocolli chiave (in particolare DNS, BGP e IPv6), il funzionamento del sistema dei nomi di dominio (come il funzionamento di tutti i domini di primo livello) e il funzionamento della zona root.

(24) Il compito di base dell'ENISA è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva (UE) 2016/1148 e degli altri strumenti giuridici pertinenti che presentano aspetti relativi alla cibersicurezza, che è essenziale per rafforzare la ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.

(25) L'ENISA dovrebbe assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare le minacce e gli incidenti e relativi alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — «CSIRT») nazionali e dell'Unione previsti dalla direttiva (UE) 2016/1148 perché raggiungano un livello comune elevato di maturità nell'Unione. Le attività svolte dall'ENISA in relazione alle capacità operative degli Stati membri dovrebbero sostenere attivamente le azioni intraprese dagli Stati membri per adempiere agli obblighi derivanti dalla direttiva (UE) 2016/1148 e non dovrebbero pertanto sostituirsi a esse.

(26) L'ENISA dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie in materia di sicurezza delle reti e dei sistemi informativi a livello di Unione e, su richiesta, a livello di Stati membri, in particolare per quanto riguarda la cibersicurezza, e dovrebbe promuovere la diffusione di tali strategie e seguirne il progresso della loro attuazione. Dovrebbe inoltre contribuire a soddisfare la necessità di formazione e materiale formativo, comprese le necessità degli enti pubblici e, se del caso, in larga misura «formare i formatori», basandosi sul quadro delle competenze digitali per i cittadini al fine di assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nello sviluppo di capacità di formazione autonome.

(27) L'ENISA dovrebbe sostenere gli Stati membri nel campo della sensibilizzazione e dell'istruzione in materia di cibersicurezza facilitando un coordinamento più stretto e lo scambio delle migliori pratiche tra Stati membri. Tale sostegno potrebbe consistere nello sviluppo di una rete di punti di contatto nazionali in materia di istruzione e di una piattaforma di formazione sulla cibersicurezza. La rete di punti di contatto nazionali in materia di istruzione potrebbe operare nel quadro della rete dei funzionari nazionali di collegamento e costituire un punto di partenza per il coordinamento futuro all'interno degli Stati membri.

(28) L'ENISA dovrebbe assistere il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 nell'esecuzione dei suoi compiti, in particolare mettendo a disposizione competenze, fornendo consulenze e agevolando lo scambio di migliori pratiche, tra l'altro per quanto riguarda l'individuazione degli operatori di servizi essenziali da parte degli Stati membri, nonché in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

(29) Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, in particolare per sostenere la protezione delle infrastrutture critiche, l'ENISA dovrebbe sostenere la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili e sulle procedure, nonché fornendo orientamenti su come affrontare le questioni normative relative alla condivisione delle informazioni, ad esempio agevolando la creazione di centri settoriali di condivisione e di analisi delle informazioni.

(30) Considerando il potenziale impatto negativo delle vulnerabilità nei prodotti TIC, servizi TIC e processi TIC è in costante aumento, nella riduzione del rischio totale connesso alla cibersicurezza è di considerevole importanza individuare ed eliminare tali vulnerabilità. È comprovato che la cooperazione tra le organizzazioni, i fabbricanti o i fornitori di prodotti TIC, servizi TIC e processi TIC vulnerabili, i membri della comunità di ricerca in materia di cibersicurezza e le autorità che individuano tali vulnerabilità accresce considerevolmente il tasso di individuazione e di eliminazione delle vulnerabilità nei prodotti TIC, servizi TIC e processi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato di cooperazione in cui le vulnerabilità sono segnalate al proprietario del sistema informativo, offrendo in tal modo all'organizzazione la possibilità di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano comunicate a terze parti o al pubblico. Il processo prevede anche il coordinamento tra la parte che ha individuato le vulnerabilità e l'organizzazione per quanto riguarda la pubblicazione di dette vulnerabilità. Le politiche di gestione della divulgazione coordinata delle vulnerabilità potrebbero svolgere un ruolo importante negli sforzi degli Stati membri tesi a migliorare la cibersicurezza.

(31) L'ENISA dovrebbe aggregare e analizzare le relazioni nazionali volontariamente condivise dei CSIRT e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione istituita dall'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 (*Computer Emergency Response Team* — «CERT-UE») ([14]) allo scopo di contribuire alla definizione di procedure, lingua e terminologia comuni per lo scambio delle informazioni. In tale contesto l'ENISA dovrebbe coinvolgere il settore privato nell'ambito della direttiva (UE) 2016/1148, che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo, nella rete di gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Teams* — «rete CSIRT») istituita da tale direttiva.

(32) L'ENISA dovrebbe contribuire a una risposta a livello di Unione in caso di crisi e incidenti transfrontalieri su vasta scala relativi alla cibersicurezza. Tale compito dovrebbe essere espletato questa funzione conformemente al mandato assegnatole ai sensi del presente regolamento e a un approccio da concordarsi tra gli Stati membri nel contesto della raccomandazione (UE) 2017/1584 della Commissione ([15]) e delle conclusioni del Consiglio del 26 giugno 2018 relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala. Tale compito potrebbe comprendere la raccolta delle informazioni pertinenti e il ruolo di facilitatore tra la rete di CSIRT e la comunità tecnica nonché tra i responsabili decisionali nella gestione delle crisi. Inoltre, l'ENISA dovrebbe sostenere la cooperazione operativa tra gli Stati membri, se richiesto da uno o più Stati membri, nella gestione degli incidenti dal punto di vista tecnico, agevolando gli scambi di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'ENISA dovrebbe sostenere la cooperazione operativa sottoponendo a prova le modalità di tale cooperazione attraverso esercitazioni periodiche di cibersicurezza.

(33) Nel sostenere la cooperazione operativa, l'ENISA dovrebbe avvalersi delle competenze tecniche e operative disponibili della CERT-UE attraverso una cooperazione strutturata. Tale cooperazione strutturata potrebbe fondarsi sulle competenze dell'ENISA. Se del caso, dovrebbero essere conclusi appositi accordi tra i due soggetti per definire l'attuazione pratica di tale cooperazione ed evitare la duplicazione delle attività.

(34) Nello svolgere il suo compito di sostegno della cooperazione operativa nell'ambito della rete di CSIRT, l'ENISA dovrebbe essere in grado di assistere gli Stati membri su loro richiesta, ad esempio fornendo consulenza su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi, agevolando la gestione tecnica di incidenti aventi un impatto rilevante o sostanziale, o assicurando che minacce e incidenti informatici siano analizzati. L'ENISA dovrebbe agevolare la gestione tecnica di incidenti aventi un impatto rilevante o sostanziale, in particolare sostenendo la condivisione volontaria di soluzioni tecniche tra gli Stati membri o producendo informazioni tecniche combinate, quali soluzioni tecniche volontariamente condivise dagli Stati membri. Nella raccomandazione (UE) 2017/1584, la Commissione raccomanda agli Stati membri di cooperare in buona fede e di condividere tra loro e con l'ENISA, senza indebiti ritardi, le informazioni sugli incidenti e le crisi su vasta scala relativi alla cibersicurezza. Tali informazioni aiuterebbero ulteriormente l'ENISA nello svolgimento dei suoi compiti di sostegno alla cooperazione operativa.

(35) Nell'ambito della costante cooperazione a livello tecnico per sostenere la consapevolezza della situazione dell'Unione, l'ENISA dovrebbe elaborare periodicamente, in stretta cooperazione con gli Stati membri, una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatici, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise dai CSIRT degli Stati membri o dai punti di contatto unici in materia di sicurezza delle reti e dei sistemi informativi («punti di contatto unici») previsti dalla direttiva (UE) 2016/1148, in entrambi i casi su base volontaria, dal Centro europeo per la lotta alla criminalità informatica (*European Cybercrime Centre* — EC3) presso Europol, dalla CERT-UE e, ove necessario, dal Centro UE di situazione e di intelligence (*European Union Intelligence and Situation Centre* — EU INTCEN) presso il Servizio europeo per l'azione esterna. Tale relazione dovrebbe essere messa a disposizione del Consiglio, della Commissione, dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e della rete di CSIRT.

(36) Il sostegno dell'ENISA alle indagini tecniche ex post effettuate, su richiesta degli Stati membri interessati, sugli incidenti aventi un impatto rilevante o sostanziale dovrebbe essere incentrato sulla prevenzione degli incidenti futuri. Gli Stati membri interessati dovrebbero fornire le informazioni e l'assistenza necessarie per consentire all'ENISA di sostenere efficacemente l'indagine tecnica ex post.

([14]) GU C 12 del 13.1.2018, pag. 1.
([15]) 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).

(37) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'ENISA, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale e le informazioni pertinenti alla pubblica sicurezza.

(38) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni, agli organi e agli organismi dell'Unione, l'ENISA ha bisogno di analizzare i rischi attuali ed emergenti connessi alla cibersicurezza. A tal fine, in cooperazione con gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'ENISA dovrebbe raccogliere le informazioni pertinenti pubblicamente disponibili o volontariamente condivise, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'ENISA dovrebbe inoltre assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nell'individuazione dei rischi emergenti connessi alla cibersicurezza e nella prevenzione degli incidenti attraverso l'analisi di minacce informatiche, vulnerabilità e incidenti.

(39) Al fine di aumentare la resilienza dell'Unione, l'ENISA dovrebbe sviluppare le competenze nel campo della cibersicurezza delle infrastrutture, in particolare per sostenere i settori di cui all'allegato II della direttiva (UE) 2016/1148 e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva, fornendo consulenza, emanando orientamenti e scambiando migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'ENISA dovrebbe sviluppare e mantenere il «polo d'informazione» dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dagli organi e dagli organismi dell'Unione e nazionali. Facilitare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili misure correttive potrebbe anche aiutare gli Stati membri a rafforzare le loro capacità, ad allineare le loro pratiche migliorando così la loro resilienza generale agli attacchi informatici.

(40) L'ENISA dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza, anche per mezzo di una campagna di sensibilizzazione in tutta l'UE promuovendo l'istruzione, e a fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini, organizzazioni e imprese. L'ENISA dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni, igiene informatica e alfabetizzazione informatica comprese, a livello di cittadini, organizzazioni e imprese mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione e la pubblicazione di relazioni e orientamenti per cittadini, organizzazioni e imprese, e a migliorare il livello complessivo di preparazione e resilienza di questi. L'ENISA dovrebbe impegnarsi, inoltre, a comunicare ai consumatori le informazioni pertinenti relative ai sistemi di certificazione applicabili, ad esempio fornendo orientamenti e raccomandazioni. L'ENISA dovrebbe inoltre organizzare regolarmente, in linea con il piano d'azione per l'istruzione digitale stabilito nella comunicazione della Commissione del 17 gennaio 2018 e in cooperazione con gli Stati membri e con le istituzioni, gli organi e gli organismi dell'Unione, campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali per promuovere comportamenti online più sicuri da parte degli individui e l'alfabetizzazione digitale, di accrescere la consapevolezza circa le potenziali minacce informatiche, compresa l'attività informatica online, ad esempio *phishing*, *botnet*, frodi finanziarie e bancarie, casi di frode di dati, nonché di promuovere consigli di base in materia di autenticazione multifattoriale, *patching*, cifratura, anonimizzazione e protezione dei dati.

(41) L'ENISA dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi e sull'uso sicuro dei servizi, e dovrebbe promuovere sicurezza e privacy fin dalla progettazione a livello di Unione. Nel perseguire tale obiettivo, l'ENISA dovrebbe utilizzare le migliori pratiche ed esperienze disponibili, in particolare quelle delle istituzioni universitarie e dei ricercatori che si occupano di sicurezza informatica.

(42) Al fine di sostenere le imprese operanti nel campo della cibersicurezza, come pure gli utilizzatori delle soluzioni di cibersicurezza, l'ENISA dovrebbe sviluppare e mantenere un «osservatorio del mercato» mediante l'esecuzione di analisi periodiche e la diffusione di informazioni sulle principali tendenze del mercato della cibersicurezza, sul versante sia della domanda che dell'offerta.

(43) L'ENISA dovrebbe contribuire agli sforzi di cooperazione dell'Unione con organizzazioni internazionali come anche nell'ambito dei pertinenti quadri di cooperazione internazionale nel campo della cibersicurezza. In particolare dovrebbe contribuire, se del caso, alla cooperazione con organizzazioni quali l'OCSE, l'OSCE e la NATO. Tale cooperazione potrebbe comprendere, tra l'altro, esercitazioni congiunte di cibersicurezza e il coordinamento congiunto della risposta agli incidenti. Occorre che tali attività si svolgano nel pieno rispetto dei principi di inclusività, reciprocità e autonomia decisionale dell'Unione, fatto salvo il carattere specifico della politica di sicurezza e di difesa di ciascuno Stato membro.

(44) Per conseguire appieno i propri obiettivi, l'ENISA dovrebbe instaurare rapporti con le autorità di vigilanza dell'Unione e con altre autorità competenti nell'Unione, le istituzioni, gli organi e gli organismi pertinenti dell'Unione, compresi la CERT-UE, l'EC3, l'Agenzia europea per la difesa (AED), l'Agenzia del sistema globale di navigazione via satellite europeo (Agenzia del GNSS europeo), l'organismo dei regolatori europei delle comunicazioni elettroniche (*Body of European Regulators for Electronic Communications* — BEREC), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE), il comitato europeo per la protezione dei dati (*European Data Protection Board* — EDPB), l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (*Agency for the Cooperation of Energy Regulators* — ACER), l'Agenzia europea per la sicurezza aerea (*European Union Aviation Safety Agency* — EASA) e tutte le agenzie dell'Unione coinvolte nella cibersicurezza. L'ENISA dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo di consulenza dell'ENISA. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'ENISA dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

(45) Si potrebbero istituire partenariati con le istituzioni universitarie che hanno avviato iniziative di ricerca nei settori interessati e vi dovrebbero essere opportuni canali per il contributo delle organizzazioni dei consumatori e di altre organizzazioni, che dovrebbe essere preso in considerazione.

(46) L'ENISA, nel suo ruolo di segretariato della rete di CSIRT, dovrebbe sostenere i CSIRT degli Stati membri e la CERT-UE nella cooperazione operativa in relazione a tutte le pertinenti funzioni della rete di CSIRT di cui alla direttiva (UE) 2016/1148. Inoltre, l'ENISA dovrebbe promuovere e sostenere la cooperazione tra i CSIRT interessati in caso di incidenti, attacchi o perturbazioni delle reti o delle infrastrutture della cui gestione o protezione sono responsabili i CSIRT e nei quali siano o possano essere coinvolti almeno due CSIRT, tenendo debitamente conto delle procedure operative standard della rete di CSIRT.

(47) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti, l'ENISA dovrebbe organizzare periodicamente esercitazioni di cibersicurezza a livello di Unione e, su loro richiesta, assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione e nell'organizzazione delle esercitazioni. Ogni due anni dovrebbero essere organizzate esercitazioni globali su vasta scala che comprendano elementi tecnici, operativi o strategici. L'ENISA dovrebbe poter inoltre organizzare periodicamente esercitazioni meno estese con lo stesso obiettivo di rafforzare la preparazione dell'Unione nel rispondere agli incidenti.

(48) L'ENISA dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'Unione in tale campo. L'ENISA dovrebbe basarsi sulle migliori pratiche esistenti e promuovere la diffusione della certificazione della cibersicurezza nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione (quadro europeo di certificazione della cibersicurezza) al fine di aumentare la trasparenza dell'affidabilità dei prodotti TIC, servizi TIC e processi TIC in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.

(49) Strategie efficaci in materia di cibersicurezza dovrebbero essere basate su buoni metodi di valutazione dei rischi, sia nel settore pubblico che in quello privato. I metodi di valutazione dei rischi sono utilizzati a diversi livelli, e non esiste una prassi comune per quanto riguarda le modalità per una loro applicazione efficiente. La promozione e lo sviluppo di migliori pratiche per la valutazione dei rischi e per soluzioni interoperabili per la loro gestione nelle organizzazioni del settore pubblico e del settore privato aumenteranno il livello di cibersicurezza nell'Unione. A tal fine, l'ENISA dovrebbe sostenere la cooperazione tra i portatori di interessi a livello di Unione e facilitare il loro impegno nella definizione e nella diffusione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza misurabile di prodotti, sistemi, reti e servizi elettronici che, insieme ai software, costituiscono le reti e i sistemi informativi.

(50) L'ENISA dovrebbe incoraggiare gli Stati membri, i fabbricanti o i fornitori prodotti TIC, servizi TIC o processi TIC a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di Internet possano adottare le misure necessarie a garantire la propria cibersicurezza e incentivarli a farlo. In particolare, i fabbricanti e i fornitori di servizi di prodotti TIC, servizi TIC o processi TIC dovrebbero fornire tutti i necessari aggiornamenti e richiamare, ritirare o riciclare i prodotti TIC, i servizi TIC o i processi TIC non conformi alle norme in materia di cibersicurezza, mentre gli importatori e i distributori dovrebbero garantire che i prodotti TIC, servizi TIC e processi TIC che immettono sul mercato dell'Unione siano conformi ai requisiti applicabili e non presentino rischi per i consumatori dell'Unione.

(51) In collaborazione con le autorità competenti, l'ENISA dovrebbe poter diffondere informazioni sul livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC offerti nel mercato interno e dovrebbe rivolgere avvertimenti ai fabbricanti e ai fornitori di prodotti TIC, servizi TIC o processi TIC imponendo loro di migliorare la sicurezza dei loro prodotti TIC, servizi TIC o processi TIC, ivi inclusa la cibersicurezza.

(52) L'ENISA dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, agli organi e agli organismi dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca e le priorità nel campo della cibersicurezza. Per individuare le esigenze e priorità in materia di ricerca, l'ENISA dovrebbe inoltre consultare i pertinenti gruppi di utenti. Più nello specifico si potrebbe istituire una cooperazione con il Consiglio europeo della ricerca, con l'Istituto europeo di innovazione e tecnologia e con l'Istituto dell'Unione europea per gli studi sulla sicurezza.

(53) L'ENISA dovrebbe consultare regolarmente le organizzazioni di normazione, in particolare quelle europee, nell'elaborare i sistemi europei di certificazione della cibersicurezza.

(54) Le minacce informatiche sono un problema globale. È necessaria una più stretta cooperazione internazionale per migliorare le norme di cibersicurezza, anche definendo norme di comportamento, ed è necessaria l'adozione di codici di condotta comuni, l'utilizzo di norme internazionali e la condivisione di informazioni, promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'ENISA dovrebbe sostenere una partecipazione e una cooperazione maggiori dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo le competenze e le analisi necessarie alle istituzioni, agli organi e agli organismi dell'Unione competenti, se del caso.

(55) L'ENISA dovrebbe essere in grado di rispondere alle richieste specifiche di consulenza e di assistenza inoltrate dagli Stati membri e dalle istituzioni, dagli organi e dagli organismi dell'Unione su materie che rientrano nei suoi obiettivi.

(56) È ragionevole e raccomandabile applicare taluni principi per la gestione dell'ENISA al fine di conformarsi alla dichiarazione congiunta e nell'approccio comune concordati nel luglio 2012 dal gruppo di lavoro interistituzionale sulle agenzie decentrate dell'Unione, il cui obiettivo è di razionalizzare le attività delle agenzie decentrate e di migliorarne l'efficacia. Le raccomandazioni contenute nella dichiarazione congiunta e nell'approccio comune dovrebbero riflettersi, se del caso, nei programmi di lavoro dell'ENISA, nelle sue valutazioni e nelle sue prassi di informazione e amministrazione.

(57) Il consiglio di amministrazione, composto dai rappresentanti degli Stati membri e della Commissione, dovrebbe stabilire l'orientamento generale delle operazioni dell'ENISA e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificare l'esecuzione del bilancio, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'ENISA, adottare il documento unico di programmazione dell'ENISA, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione e alla conclusione del suo mandato.

(58) Per garantire il funzionamento corretto ed efficace dell'ENISA, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze professionali e di esperienza adeguate. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori.

(59) Il corretto funzionamento dell'ENISA esige che il direttore esecutivo sia nominato in base ai meriti e alle comprovate abilità amministrative e manageriali, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza. Le funzioni del direttore esecutivo dovrebbero essere svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'ENISA e adottare tutte le misure necessarie a garantirne l'adeguata attuazione. Il direttore esecutivo dovrebbe redigere una relazione annuale da trasmettere al consiglio di amministrazione che includa l'attuazione del programma di lavoro annuale dell'ENISA, fornire un progetto di stato di previsione delle entrate e delle spese dell'ENISA e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura scientifica, tecnica, giuridica o socio-economica. Si considera necessaria l'istituzione di un gruppo ad hoc soprattutto per quanto riguarda la preparazione di una specifica proposta di sistema europeo di certificazione della cibersicurezza («proposta di sistema»). Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti

secondo i più elevati standard di competenza, con l'intento di garantire un equilibrio di genere e un equilibrio adeguato, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e il settore privato, tra cui le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

(60) Il comitato esecutivo dovrebbe contribuire al funzionamento efficace del consiglio di amministrazione. Nel quadro dei lavori preparatori relativi alle decisioni del consiglio di amministrazione, il comitato esecutivo dovrebbe esaminare dettagliatamente le informazioni pertinenti, valutare le opzioni disponibili e fornire consulenza e soluzioni per la preparazione delle decisioni del consiglio di amministrazione.

(61) È opportuno che l'ENISA disponga di un gruppo consultivo ENISA come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo consultivo ENISA, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'ENISA. Il gruppo consultivo ENISA dovrebbe essere consultato in particolare in merito al progetto di programma di lavoro annuale dell'ENISA. La composizione del gruppo consultivo ENISA e i compiti assegnatigli dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'ENISA.

(62) È opportuno istituire il gruppo dei portatori di interessi per la certificazione della cibersicurezza al fine di aiutare l'ENISA e la Commissione ad agevolare la consultazione con i pertinenti portatori di interessi. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza dovrebbe essere costituito da membri che rappresentino il settore in proporzione equilibrata, sul versante sia della domanda che dell'offerta di prodotti TIC e servizi TIC, fra cui in particolare le PMI, i fornitori di servizi digitali, gli organismi europei e internazionali di normazione, gli organismi nazionali di accreditamento, le autorità di controllo preposte alla protezione dei dati e gli organismi di valutazione della conformità a norma del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([16]), e le università, nonché le organizzazioni dei consumatori.

(63) L'ENISA dovrebbe disporre di regole relative alla prevenzione e alla gestione dei conflitti di interessi. L'ENISA dovrebbe inoltre applicare le disposizioni pertinenti dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([17]). Il trattamento dei dati personali da parte dell'ENISA dovrebbe avvenire in conformità del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([18]). È opportuno che l'ENISA si conformi alle disposizioni applicabili alle istituzioni, gli organi e gli organismi dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate UE (ICUE).

(64) Per garantire all'ENISA piena autonomia e indipendenza e consentirle di svolgere compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'ENISA. Un idoneo bilancio è essenziale per garantire che l'ENISA disponga di capacità sufficienti ad adempiere i suoi crescenti compiti e conseguire i suoi obiettivi nella loro totalità. La maggior parte del personale dell'ENISA dovrebbe essere impiegata nell'attuazione operativa del suo mandato. Allo Stato membro ospitante, e a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente al bilancio dell'ENISA. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della rendicontabilità, la revisione contabile dell'ENISA dovrebbe essere svolta dalla Corte dei conti.

(65) La certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti TIC, servizi TIC e processi TIC e nell'accrescere la fiducia negli stessi. Il mercato unico digitale, in particolare l'economia dei dati e l'Internet degli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un determinato livello di cibersicurezza. Le automobili connesse e automatizzate, i dispositivi medici elettronici, i sistemi di controllo per l'automazione industriale e le reti elettriche intelligenti sono solo alcuni esempi di settori in cui la certificazione è già ampiamente utilizzata o sarà probabilmente utilizzata in un prossimo futuro. La certificazione della cibersicurezza riveste un'importanza fondamentale anche nei settori disciplinati dalla direttiva (UE) 2016/1148.

([16]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

([17]) 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).

([18]) 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).

(66) Nella comunicazione del 2016 dal titolo «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza» la Commissione ha sottolineato la necessità di prodotti e soluzioni di alta qualità, a costi contenuti e interoperabili. L'offerta di prodotti, servizi TIC e processi TIC nel mercato unico resta molto frammentata dal punto di vista geografico. La causa di tale frammentazione va ravvisata nel fatto che il settore della cibersicurezza in Europa si è sviluppato soprattutto in risposta alla domanda pubblica nazionale. Inoltre, l'assenza di soluzioni interoperabili (norme tecniche), di pratiche e di meccanismi di certificazione nell'Unione è un'altra delle lacune che influisce sul mercato unico nel campo della cibersicurezza. Ciò incide negativamente sulla competitività delle imprese europee a livello nazionale, dell'Unione e mondiale. Allo stesso tempo limita la gamma di tecnologie di cibersicurezza valide e utilizzabili a cui cittadini e imprese hanno accesso. Anche nella comunicazione del 2017 sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale — Un mercato unico digitale connesso per tutti, la Commissione ha evidenziato la necessità di prodotti e sistemi connessi sicuri e ha dichiarato che la creazione di un quadro europeo di sicurezza delle TIC che definisca regole su come organizzare la certificazione della sicurezza delle TIC nell'Unione potrebbe sia preservare la fiducia nei confronti di Internet sia permettere di affrontare l'attuale frammentazione del mercato interno.

(67) Attualmente la certificazione della cibersicurezza di prodotti TIC, servizi TIC e processi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dal settore. In tale contesto, un certificato rilasciato da un'autorità nazionale di certificazione della cibersicurezza non è, in linea di principio, riconosciuto negli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti TIC, servizi TIC e processi TIC nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti, il che aumenta i relativi costi. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'Internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo, impedendo meccanismi di riconoscimento reciproco nell'Unione.

(68) Sono stati compiuti sforzi finalizzati a garantire il reciproco riconoscimento dei certificati all'interno dell'Unione. Il loro successo tuttavia è stato solo parziale. L'esempio più importante in tal senso è l'accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (*Senior Officials Group — Information Systems Security* — SOG-IS). Sebbene rappresenti il più importante modello di cooperazione e di riconoscimento reciproco nel campo della certificazione della sicurezza, il SOG-IS comprende solo alcuni Stati membri. Ciò ha limitato l'efficacia dell'ARR del SOG-IS dal punto di vista del mercato interno.

(69) È pertanto necessario adottare un approccio comune e definire un quadro europeo di certificazione della cibersicurezza che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e che consenta di riconoscere e utilizzare i certificati europei di cibersicurezza e le dichiarazioni UE di conformità per i prodotti TIC, i servizi TIC o i processi TIC in tutti gli Stati membri. In questo senso, è essenziale basarsi sui sistemi nazionali e internazionali esistenti, nonché sui sistemi di riconoscimento reciproco, in particolare il SOG-IS, e consentire un'agevole transizione dai sistemi esistenti funzionanti nel loro ambito verso sistemi basati sul nuovo quadro europeo di certificazione della cibersicurezza. Il quadro europeo di certificazione della cibersicurezza dovrebbe avere un duplice obiettivo. In primo luogo dovrebbe contribuire ad aumentare la fiducia nei prodotti TIC, servizi TIC e processi TIC che sono stati certificati in base a detti sistemi europei di certificazione della cibersicurezza. In secondo luogo, dovrebbe evitare il proliferare di sistemi di certificazione nazionali della cibersicurezza confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi europei di certificazione della cibersicurezza dovrebbero essere non discriminatori e basati su norme europee o internazionali, a meno che tali norme non siano inefficaci o inadeguate ai fini del conseguimento dei legittimi obiettivi dell'Unione in tale ambito.

(70) Il quadro europeo di certificazione della cibersicurezza dovrebbe essere istituito in modo uniforme in tutti gli Stati membri, in modo da evitare la scelta della certificazione più vantaggiosa in base ai diversi livelli di rigore nei vari Stati membri.

(71) I sistemi europei di certificazione della cibersicurezza dovrebbero essere basati sui sistemi già esistenti a livello nazionale e internazionale e, se necessario, sulle specifiche tecniche di forum e consorzi, partendo dai loro punti di forza attuali e analizzando e correggendo i punti deboli.

(72) Occorrono soluzioni flessibili di cibersicurezza affinché il settore resti un passo avanti rispetto alle minacce, per cui qualsiasi sistema di certificazione dovrebbe essere ideato in modo tale da evitare il rischio di una rapida obsolescenza.

(73) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti, servizi TIC e processi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di certificazione della cibersicurezza e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dal settore o da altre organizzazioni private non dovrebbero rientrare nell'ambito di applicazione del presente regolamento. Tuttavia, gli organismi che li gestiscono dovrebbero poter proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo di certificazione della cibersicurezza.

(74) Le disposizioni del presente regolamento dovrebbero lasciare impregiudicato il diritto dell'Unione che prevede regole specifiche sulla certificazione di prodotti TIC, servizi TIC e processi TIC. In particolare, il regolamento (UE) 2016/679 stabilisce disposizioni per l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali meccanismi di certificazione e sigilli e marchi di protezione dei dati dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati dei prodotti e dei servizi. Il presente regolamento lascia impregiudicata la certificazione delle operazioni di trattamento dei dati nel quadro del regolamento (UE) 2016/679, anche nel caso in cui tali operazioni siano integrate nei TIC, servizi TIC e processi TIC.

(75) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti TIC, servizi TIC e processi TIC certificati nel loro ambito siano conformi a determinati requisiti volti a proteggere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o delle funzioni di o dei servizi offerti da o accessibili tramite tali prodotti, servizi e processi per tutto il loro ciclo di vita. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti TIC, servizi TIC e processi TIC nel presente regolamento. I prodotti TIC, servizi TIC e processi TIC e le esigenze di cibersicurezza ad essi relative sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, che dovrebbe essere integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento della progettazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui conseguire tali obiettivi nei prodotti TIC, servizi TIC e processi TIC specifici dovrebbero quindi essere ulteriormente specificate in modo dettagliato per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche in assenza di norme appropriate.

(76) Le specifiche tecniche da usare nei sistemi europei di certificazione della cibersicurezza dovrebbero rispettare i requisiti principi enunciati nell'allegato II del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([19]). In casi debitamente giustificati, tuttavia, si potrebbe ritenere necessario discostarsi da detti requisiti qualora le specifiche tecniche siano da usare in un sistema europeo di certificazione della cibersicurezza che fa riferimento a un livello di affidabilità elevato. Le motivazioni di tali scostamenti dovrebbero essere rese pubbliche.

(77) La valutazione della conformità è la procedura volta a valutare se siano stati rispettati i requisiti specifici connessi a un prodotto TIC, servizio TIC o processo TIC. Tale procedura è effettuata da un soggetto terzo indipendente, diverso dal fabbricante o dal fornitore del prodotto TIC, servizio TIC o processo TIC oggetto di valutazione. Il rilascio di un certificato europeo di cibersicurezza è in linea con la procedura di valutazione di un prodotto TIC, servizio TIC o processo TIC. Un certificato europeo di cibersicurezza dovrebbe essere rilasciato qualora la valutazione di un prodotto TIC, servizio TIC o processo TIC dia esito positivo. In funzione del livello di affidabilità, il sistema europeo di certificazione della cibersicurezza dovrebbe specificare se il certificato europeo di cibersicurezza deve essere rilasciato da un organismo pubblico o privato. La valutazione della conformità e la certificazione non possono garantire di per sé la cibersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati. Si tratta piuttosto di procedure e metodologie tecniche volte ad attestare che i prodotti TIC, servizi TIC e processi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio nelle norme tecniche.

(78) La scelta della certificazione appropriata e dei relativi requisiti di sicurezza da parte degli utenti dei certificati europei di cibersicurezza dovrebbe fondarsi su un'analisi dei rischi associati all'uso di un prodotto TIC, servizio TIC o processo TIC. Conseguentemente, il livello di affidabilità dovrebbe essere commisurato al livello del rischio associato al previsto uso di un prodotto TIC, servizio TIC o processo TIC.

([19]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

(79) I sistemi europei di certificazione della cibersicurezza potrebbero prevedere che la valutazione della conformità sia effettuata sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC o processi TIC («autovalutazione della conformità»). In tal caso dovrebbe essere sufficiente che il fabbricante o il fornitore di prodotti TIC, servizi TIC o processi TIC effettui direttamente tutti i controlli per garantire che i prodotti TIC, servizi TIC o processi TIC siano conformi al sistema europeo di certificazione della cibersicurezza. L'autovalutazione della conformità dovrebbe essere considerata idonea per prodotti TIC, servizi TIC o processi TIC a bassa complessità che presentano un basso livello di rischio per l'interesse pubblico, ad esempio progettazione e meccanismi di produzione semplici. Inoltre, l'autovalutazione della conformità dovrebbe essere consentita solo per i prodotti TIC, servizi TIC o processi TIC che corrispondono al livello di affidabilità «di base».

(80) I sistemi europei di certificazione della cibersicurezza potrebbero prevedere sia l'autovalutazione della conformità sia la certificazione di prodotti TIC, servizi TIC e processi TIC. In tale caso, il sistema dovrebbe comprendere mezzi chiari e comprensibili che consentano ai consumatori o altri utenti di distinguere tra i prodotti TIC, servizi TIC o processi TIC riguardo ai quali il fabbricante o fornitore di prodotti TIC, servizi TIC e processi TIC è responsabile della valutazione di prodotti TIC, servizi TIC e processi TIC certificati da terzi.

(81) I fabbricanti o fornitori di prodotti TIC, servizi TIC o processi TIC che effettuano un'autovalutazione della conformità dovrebbero poter rilasciare e firmare la dichiarazione UE di conformità nell'ambito della procedura di valutazione della conformità. Una dichiarazione UE di conformità è un documento che attesta che un prodotto TIC, servizio TIC o processo TIC specifico è conforme ai requisiti del sistema europeo di certificazione della cibersicurezza. Rilasciando e firmando la dichiarazione UE di conformità, il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC si assume la responsabilità della conformità del prodotto TIC, servizio TIC o processo TIC con i requisiti di legge del sistema europeo di certificazione della cibersicurezza. Una copia della dichiarazione UE di conformità dovrebbe essere trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

(82) I fabbricanti o fornitori di prodotti TIC, servizi TIC o processi TIC dovrebbero mettere a disposizione della competente autorità nazionale di certificazione della cibersicurezza, per un periodo stabilito nel sistema europeo di certificazione della cibersicurezza interessato, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC, servizi TIC o processi TIC al pertinente sistema europeo di certificazione della cibersicurezza. La documentazione tecnica dovrebbe precisare i requisiti applicabili nell'ambito del sistema e riguardare la progettazione, la fabbricazione e il funzionamento del prodotto TIC, servizio TIC o processo TIC per quanto rileva ai fini dell'autovalutazione della conformità. La documentazione tecnica dovrebbe essere compilata in modo da permettere di valutare se un prodotto TIC, servizio TIC o processo TIC sia conforme ai requisiti applicabili nell'ambito di tale sistema.

(83) La governance del quadro europeo di certificazione della cibersicurezza tiene conto della partecipazione degli Stati membri e dell'adeguato coinvolgimento dei portatori di interessi e stabilisce il ruolo della Commissione durante l'intero processo di pianificazione e di proposta, richiesta, preparazione, adozione e revisione dei sistemi europei di certificazione della cibersicurezza.

(84) È opportuno che la Commissione prepari, con il sostegno del gruppo europeo per la certificazione della cibersicurezza (*European Cybersecurity Certification Group* — «ECCG») e del gruppo dei portatori di interessi per la certificazione della cibersicurezza e dopo una consultazione ampia e aperta, un programma di lavoro progressivo dell'Unione per i sistemi europei di certificazione della cibersicurezza e lo pubblichi sotto forma di strumento non vincolante. Il programma di lavoro progressivo dell'Unione dovrebbe consistere in un documento strategico atto a consentire al settore, alle autorità nazionali e agli organismi di normazione, in particolare, di prepararsi in anticipo ai futuri sistemi europei di certificazione della sicurezza. Il programma di lavoro progressivo dell'Unione dovrebbe includere una panoramica pluriennale delle richieste di proposte di sistemi che la Commissione intende presentare all'ENISA ai fini della loro preparazione in base a motivi specifici. La Commissione dovrebbe tenere conto del programma di lavoro progressivo dell'Unione nella preparazione del suo programma continuativo per la normazione delle TIC e delle richieste di normazione alle organizzazioni europee di normazione. In considerazione della rapida introduzione e diffusione di nuove tecnologie, dell'emergere di rischi connessi alla cibersicurezza prima sconosciuti e degli sviluppi legislativi e del mercato, è opportuno autorizzare la Commissione o l'ECCG a chiedere all'ENISA di preparare proposte di sistemi che non siano stati previsti nel programma di lavoro progressivo dell'Unione. In siffatti casi, la Commissione e l'ECCG dovrebbero inoltre valutare la necessità di tale richiesta, tenendo conto degli scopi e obiettivi generali del presente regolamento e la necessità di assicurare la continuità per quanto riguarda la pianificazione e l'uso delle risorse da parte dell'ENISA.

A seguito di una simile richiesta, l'ENISA dovrebbe preparare senza indebiti ritardi le proposte di sistemi per prodotti TIC, servizi TIC e processi TIC specifici. La Commissione dovrebbe valutare l'impatto positivo e negativo della sua richiesta sullo specifico mercato interessato, in particolare sulle PMI, sull'innovazione, sugli ostacoli all'accesso a tale mercato e sui costi per gli utenti finali. La Commissione, sulla base dei sistemi preparati dall'ENISA, dovrebbe essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza fissati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Detti elementi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti TIC, servizi TIC e processi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato («di base», «sostanziale» o «elevato»), nonché i livelli di valutazione ove applicabili. L'ENISA dovrebbe poter respingere, in casi debitamente giustificati, una richiesta dell'ECCG. Tali decisioni dovrebbero essere assunte dal consiglio di amministrazione e dovrebbero essere debitamente motivate.

(85) L'ENISA dovrebbe gestire un sito web che fornisca informazioni sui sistemi europei di certificazione della cibersicurezza e che li pubblicizzi, in cui figurino, tra l'altro, le richieste di preparazione di una proposta di sistema e il riscontro ricevuto nella procedura di consultazione effettuata dall'ENISA durante la fase di preparazione. Il sito web dovrebbe anche fornire informazioni sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità rilasciati ai sensi del presente regolamento, incluse le informazioni sulla revoca e sulla scadenza di tali certificati e dichiarazioni. Il sito web dovrebbe inoltre indicare i sistemi nazionali di certificazione della cibersicurezza che sono stati sostituiti da un sistema europeo di certificazione della cibersicurezza.

(86) Il livello di affidabilità di un sistema europeo di certificazione è la base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfi i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza. Allo scopo di garantire la coerenza del quadro europeo di certificazione della cibersicurezza, un sistema europeo di certificazione della cibersicurezza dovrebbe poter specificare i livelli di affidabilità per i certificati europei di cibersicurezza e le dichiarazioni UE di conformità rilasciati nell'ambito di detto sistema. Ciascun certificato europeo di cibersicurezza potrebbe far riferimento a uno dei livelli di affidabilità: «di base», «sostanziale» o «elevato», mentre la dichiarazione UE di conformità potrebbe far riferimento solo al livello di affidabilità «di base». I livelli di affidabilità fornirebbero il rigore e la specificità corrispondenti della valutazione del prodotto TIC, servizio TIC o processo TIC e sarebbero caratterizzati in riferimento alle specifiche tecniche, norme e procedure correlate, tra cui i controlli tecnici, l'obiettivo delle quali è attenuare o prevenire gli incidenti. Ciascun livello di affidabilità dovrebbe essere coerente nei vari settori in cui la certificazione si applica.

(87) Un sistema europeo di certificazione della cibersicurezza potrebbe precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia usata. I livelli di valutazione dovrebbero corrispondere a uno dei livelli di affidabilità ed essere associati a un'idonea combinazione di componenti dell'affidabilità. Per tutti i livelli di affidabilità, il prodotto TIC, servizio TIC o processo TIC dovrebbe contenere alcune funzioni sicure, specificate nel sistema, che possono comprendere una configurazione sicura già predisposta in fabbrica, un codice firmato, aggiornamenti sicuri e tecniche utilizzate per ostacolare lo sfruttamento delle vulnerabilità (*exploit mitigations*) nonché la piena protezione della memoria a impilaggio o della memoria *heap*. Dette funzioni dovrebbero essere soggette a sviluppo e manutenzione utilizzando approcci allo sviluppo centrati sulla sicurezza e strumenti ad essi associati onde assicurare che meccanismi efficaci di software e di hardware siano inclusi in maniera affidabile.

(88) Per il livello di affidabilità «di base», la valutazione dovrebbe essere guidata almeno dai seguenti componenti di affidabilità: la valutazione dovrebbe comprendere almeno un riesame della documentazione tecnica del prodotto TIC, servizio TIC o processo TIC da parte dell'organismo di valutazione della conformità. Se la certificazione comprende processi TIC, dovrebbe essere soggetto a riesame tecnico anche il processo usato per la progettazione, lo sviluppo e la manutenzione del prodotto TIC o servizio TIC. Se un sistema europeo di certificazione della cibersicurezza prevede un'autovalutazione della conformità, dovrebbe essere sufficiente che il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC abbia effettuato un'autovalutazione della conformità del prodotto TIC, servizio TIC o processo TIC al sistema di certificazione.

(89) Per il livello di affidabilità «sostanziale», la valutazione, oltre ai requisiti per il livello di affidabilità «di base», dovrebbe essere guidata almeno dalla verifica della conformità delle funzionalità di sicurezza del prodotto TIC, servizio TIC o processo TIC alla documentazione tecnica ad esso relativa.

(90) Per il livello di affidabilità «elevato», la valutazione, oltre ai criteri requisiti per il livello di affidabilità «sostanziale», dovrebbe essere guidata almeno da un test di efficacia che accerti la resistenza delle funzionalità di sicurezza di un prodotto TIC, servizio TIC o processo TIC nei confronti di complessi ciberattacchi perpetrati da persone che dispongono di abilità e risorse significative.

(91) Il ricorso alla certificazione europea della cibersicurezza e alle dichiarazioni UE di conformità dovrebbe restare volontario, salvo disposizioni contrarie previste dal diritto dell'Unione o dalla normativa degli Stati membri adottata in conformità del diritto dell'Unione. In mancanza di un diritto dell'Unione armonizzato, gli Stati membri possono adottare regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cibersicurezza in virtù della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([20]). Gli Stati membri ricorrono anche alla certificazione europea della cibersicurezza nell'ambito degli appalti pubblici e della direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([21]).

(92) In alcuni settori potrebbe essere necessario in futuro imporre specifici requisiti di cibersicurezza e rendere obbligatoria la relativa certificazione in relazione a taluni prodotti TIC, servizi TIC o processi TIC, al fine di aumentare il livello di cibersicurezza nell'Unione. La Commissione dovrebbe vigilare periodicamente sull'impatto dei sistemi europei di certificazione della cibersicurezza adottati sulla disponibilità di prodotti TIC, servizi TIC e processi TIC sicuri nel mercato interno e valutare periodicamente il livello di utilizzo dei sistemi di certificazione da parte dei fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC nell'Unione. L'efficacia dei sistemi europei di certificazione della cibersicurezza e l'opportunità di rendere obbligatori sistemi specifici dovrebbero essere valutate alla luce della normativa dell'Unione in materia di cibersicurezza, in particolare la direttiva (UE) 2016/1148, tenendo in considerazione la sicurezza delle reti e dei sistemi informativi utilizzati dagli operatori di servizi essenziali.

(93) I certificati europei di cibersicurezza e le dichiarazioni UE di conformità dovrebbero aiutare gli utenti finali a compiere scelte consapevoli. I prodotti TIC, servizi TIC e processi TIC che siano stati certificati o per i quali sia stata rilasciata una dichiarazione UE di conformità dovrebbero pertanto essere accompagnati da informazioni strutturate adeguate al livello tecnico atteso nell'utente finale previsto. Tutte queste informazioni dovrebbero essere disponibili online e, ove opportuno, in forma fisica. L'utente finale dovrebbe avere accesso alle informazioni relative al numero di riferimento del sistema di certificazione, al livello di affidabilità, alla descrizione dei rischi connessi alla cibersicurezza associati al prodotto TIC, servizio TIC o processo TIC, e all'autorità o organismo che ha rilasciato il certificato, o dovrebbe poter ottenere una copia del certificato europeo di cibersicurezza. Inoltre, l'utente finale dovrebbe essere informato della politica di assistenza in materia di cibersicurezza —ossia per quanto tempo l'utente finale può aspettarsi di ricevere aggiornamenti o patch per la cibersicurezza — del fabbricante o fornitore di prodotti TIC, servizi TIC e processi TIC. Se del caso, dovrebbero essere forniti orientamenti sulle azioni da compiere o sui parametri che l'utente finale può applicare per mantenere o aumentare la cibersicurezza del prodotto TIC o del servizio TIC e informazioni di contatto del punto di contatto unico a cui fare capo e da cui ricevere assistenza in caso di ciberattacchi (oltre alle segnalazioni automatiche). Tali informazioni dovrebbero essere aggiornate periodicamente e rese disponibili su un sito web che fornisca informazioni sui sistemi europei di certificazione della cibersicurezza.

(94) Al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti TIC, servizi TIC o processi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere da una data stabilita dalla Commissione mediante atti di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione della cibersicurezza di prodotti TIC, servizi TIC o processi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza in vigore. Non si dovrebbe tuttavia impedire agli Stati membri di adottare o mantenere in vigore sistemi nazionali di certificazione della cibersicurezza per motivi di sicurezza nazionale. Gli Stati membri dovrebbero informare la Commissione e l'ECCG dell'eventuale intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza. La Commissione e l'ECCG dovrebbero valutare l'impatto dei nuovi sistemi nazionali di certificazione della cibersicurezza sul corretto funzionamento del mercato interno, tenendo conto anche dell'eventuale interesse strategico di richiedere invece un sistema europeo di certificazione della cibersicurezza.

(95) I sistemi europei di certificazione della cibersicurezza sono volti ad armonizzare nell'Unione le pratiche in tale settore. Devono contribuire ad accrescere il livello di cibersicurezza nell'Unione. La progettazione dei sistemi europei di certificazione della cibersicurezza dovrebbe tener conto delle innovazioni nel campo della cibersicurezza e consentirne lo sviluppo.

([20]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([21]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014 sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

(96) I sistemi europei di certificazione della cibersicurezza dovrebbero tener conto degli attuali metodi di sviluppo di software e hardware e, in particolare, dell'impatto di frequenti aggiornamenti del software e del firmware sui singoli certificati europei di cibersicurezza. I sistemi europei di certificazione della cibersicurezza dovrebbero specificare le condizioni alle quali un aggiornamento possa rendere necessario sottoporre nuovamente a certificazione un prodotto TIC, servizio TIC o processo TIC oppure ridurre l'ambito di applicazione di uno specifico certificato europeo di cibersicurezza, tenuto conto dei possibili effetti negativi dell'aggiornamento sulla conformità ai requisiti di sicurezza del certificato.

(97) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC dovrebbero poter presentare domande di certificazione dei loro prodotti TIC, servizi TIC e processi TIC all'organismo di valutazione della conformità di propria scelta, ovunque nell'Unione. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo nazionale di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni e dovrebbe essere rinnovato alle stesse condizioni, purché l'organismo di valutazione della conformità continui a soddisfare i requisiti. Gli organismi di accreditamento dovrebbero limitare, sospendere o revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono state, o non sono più, soddisfatte o se l'organismo di valutazione della conformità viola le disposizioni del presente regolamento.

(98) Riferimenti nella legislazione nazionale a norme nazionali che non sono più applicabili a seguito dell'entrata in vigore di un sistema europeo di certificazione della cibersicurezza possono costituire una fonte di confusione. Gli Stati membri dovrebbero quindi tener conto dell'adozione di un sistema di certificazione europeo della cibersicurezza nella propria legislazione nazionale.

(99) Al fine di ottenere norme equivalenti in tutta l'Unione, agevolare il reciproco riconoscimento e promuovere l'accettazione generale dei certificati europei di cibersicurezza e delle dichiarazioni UE di conformità, è necessario istituire un sistema di valutazione inter pares tra le autorità nazionali di certificazione della cibersicurezza. La valutazione inter pares dovrebbe riguardare le procedure per vigilare sulla conformità dei prodotti TIC, servizi TIC e processi TIC con i certificati europei di cibersicurezza, per monitorare gli obblighi dei fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC che effettuano l'autovalutazione della conformità, per monitorare gli organismi di valutazione della conformità e l'adeguatezza delle competenze del personale degli organismi che rilasciano certificati di livello di affidabilità «elevato». La Commissione dovrebbe poter stabilire, mediante atti di esecuzione, almeno un piano quinquennale per le valutazioni inter pares e stabilire i criteri e le metodologie di funzionamento del sistema di valutazione inter pares.

(100) Fatto salvo il sistema generale di valutazione inter pares che tutte le autorità nazionali di certificazione della cibersicurezza devono istituire nell'ambito del quadro europeo di certificazione della cibersicurezza, taluni sistemi di certificazione possono includere un meccanismo di valutazione inter pares per gli organismi che rilasciano certificati europei di cibersicurezza per prodotti TIC, servizi TIC e processi TIC con un livello di affidabilità «elevato» nel quadro di tali sistemi. L'ECCG dovrebbe sostenere l'attuazione di tali meccanismi di valutazione inter pares. Le valutazioni inter pares dovrebbero in particolare valutare se gli organismi interessati svolgono i rispettivi compiti in maniera armonizzata e possono comprendere meccanismi di impugnazione. I risultati delle valutazioni inter pares dovrebbero essere resi pubblici. Gli organismi interessati possono adottare le opportune misure per adeguare le proprie prassi e competenze di conseguenza.

(101) Gli Stati membri dovrebbero designare una o più autorità nazionale di certificazione della cibersicurezza per vigilare sulla conformità agli obblighi derivanti dal presente regolamento. L'autorità nazionale di certificazione della cibersicurezza può essere un'autorità già esistente o una nuova autorità. Gli Stati membri dovrebbero altresì avere facoltà di designare, previo accordo con un altro Stato membro, una o più autorità nazionali di certificazione della cibersicurezza nel territorio di tale altro Stato membro.

(102) In particolare, l'autorità nazionale di certificazione della cibersicurezza dovrebbe monitorare e far applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC stabiliti nel suo territorio in relazione alla dichiarazione UE di conformità, assistere gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità mettendo a loro disposizione le proprie competenze e pertinenti informazioni, autorizzare gli organismi di valutazione della conformità a svolgere i loro compiti qualora questi soddisfino i requisiti supplementari previsti in un sistema europeo di certificazione della cibersicurezza e monitorare i pertinenti sviluppi nel settore della certificazione della cibersicurezza. Le autorità nazionali di certificazione della cibersicurezza dovrebbero anche trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza che sono da loro rilasciati o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità, ove tali certificati indichino

un livello di affidabilità «elevato», svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Le autorità nazionali di certificazione della cibersicurezza dovrebbero inoltre cooperare con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante la condivisione scambio di informazioni sugli eventuali prodotti TIC, servizi TIC o processi TIC non conformi ai requisiti del presente regolamento o a specifici sistemi europei di certificazione della cibersicurezza. La Commissione dovrebbe facilitare tale condivisione di informazioni mettendo a disposizione un sistema di sostegno generale delle informazioni elettroniche, ad esempio il sistema di informazione e comunicazione per la vigilanza del mercato (ICSMS) e il sistema d'informazione rapida sui prodotti non alimentari pericolosi (RAPEX) già impiegati dalle autorità di vigilanza del mercato a norma del regolamento (CE) n. 765/2008.

(103) Al fine di garantire un'applicazione coerente del quadro europeo di certificazione della cibersicurezza, dovrebbe essere costituito un ECCG costituito dai rappresentanti delle autorità nazionali di certificazione della cibersicurezza o di altre autorità nazionali competenti. I compiti principali dell'ECCG dovrebbero consistere nel consigliare e nell'assistere la Commissione nelle attività volte ad assicurare un'attuazione e un'applicazione coerenti del quadro europeo di certificazione della cibersicurezza, nell'assistere e nel cooperare strettamente con l'ENISA nella preparazione delle proposte di sistemi europei di certificazione della cibersicurezza, in casi debitamente giustificati nell'incaricare l'ENISA di preparare una proposta di sistema, nell'adottare pareri indirizzati all'ENISA in merito alle proposte di sistemi e nell'adottare pareri indirizzati sul mantenimento e la revisione degli attuali sistemi europei di certificazione della cibersicurezza. L'ECCG dovrebbe agevolare lo scambio di buone prassi e di competenze tra le diverse autorità nazionali di certificazione della cibersicurezza responsabili dell'autorizzazione degli organismi di valutazione della conformità e del rilascio dei certificati europei di cibersicurezza.

(104) Al fine di accrescere la consapevolezza e facilitare l'accettazione dei futuri sistemi europei di cibersicurezza, la Commissione può emanare orientamenti generali o settoriali in materia di cibersicurezza, ad esempio orientamenti sulle buone prassi o sul comportamento responsabile in tale ambito, sottolineando l'effetto positivo dell'utilizzo di prodotti TIC, servizi TIC e processi TIC certificati.

(105) Allo scopo di agevolare ulteriormente gli scambi e riconoscendo il carattere globale delle catene di fornitura di TIC, l'Unione può concludere, conformemente all'articolo 218 del trattato sul funzionamento dell'Unione europea (TFUE), accordi per il reciproco riconoscimento di certificati europei di cibersicurezza. La Commissione, tenuto conto del parere dell'ENISA e dell'ECCG, può raccomandare l'apertura dei negoziati pertinenti. Ciascun sistema europeo di certificazione della cibersicurezza dovrebbe prevedere condizioni specifiche per tali accordi per il reciproco riconoscimento con i paesi terzi.

(106) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([22]).

(107) La procedura d'esame dovrebbe essere utilizzata per l'adozione degli atti di esecuzione sui sistemi europei di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC; per l'adozione degli atti di esecuzione sulle modalità di conduzione delle indagini da parte dell'ENISA; per l'adozione degli atti di esecuzione su un piano di valutazione inter pares delle autorità nazionali di certificazione della cibersicurezza nonché per l'adozione degli atti di esecuzione sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di certificazione della cibersicurezza alla Commissione.

(108) L'operato dell'ENISA dovrebbe essere soggetto a una valutazione periodica e indipendente. La valutazione dovrebbe tenere conto del conseguimento degli obiettivi da parte dell'ENISA, delle sue pratiche di lavoro e della pertinenza dei suoi compiti, in particolare i compiti relativi alla cooperazione operativa a livello di Unione. La valutazione dovrebbe altresì valutare l'impatto, l'efficacia e l'efficienza del quadro europeo di certificazione della cibersicurezza. In caso di riesame, la Commissione dovrebbe valutare come possa essere rafforzato il ruolo dell'ENISA come punto di riferimento per pareri e competenze e dovrebbe anche valutare la possibilità di un ruolo dell'ENISA nel sostenere la valutazione di prodotti TIC, servizi TIC e processi e i servizi TIC di paesi terzi che non rispettano le regole dell'Unione, ove tali prodotti, servizi e processi entrino nell'Unione.

([22]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

(109) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della loro portata e dei loro effetti, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(110) Il regolamento (UE) n. 526/2013 dovrebbe essere abrogato,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento stabilisce:

a) gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA, («Agenzia dell'Unione europea per la cibersicurezza»); e

b) un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

Il quadro di cui al primo comma, lettera b), si applica fatte salve disposizioni specifiche di altri atti giuridici dell'Unione in materia di certificazione volontaria o obbligatoria.

2. Il presente regolamento fa salve le competenze degli Stati membri per quanto riguarda le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

Articolo 2

Definizioni

Ai fini del presente regolamento si intende per:

1) «cibersicurezza»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;

2) «rete e sistema informativo»: una rete e un sistema informativo quale definito all'articolo 4, punto 1), della direttiva (UE) 2016/1148;

3) «strategia nazionale per la sicurezza della rete e dei sistemi informativi»: una strategia nazionale per la sicurezza della rete e dei sistemi informativi quale definita all'articolo 4, punto 3), della direttiva (UE) 2016/1148;

4) «operatore di servizi essenziali»: un operatore di servizi essenziali quale definito all'articolo 4, punto 4), della direttiva (UE) 2016/1148;

5) «fornitore di servizio digitale»: un fornitore di servizio digitale quale definito all'articolo 4, punto 6), della direttiva (UE) 2016/1148;

6) «incidente»: un incidente quale definito all'articolo 4, punto 7), della direttiva (UE) 2016/1148;

7) «trattamento dell'incidente»: qualsiasi trattamento dell'incidente quale definito all'articolo 4, punto 8), della direttiva (UE) 2016/1148;

8) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;

9) «sistema europeo di certificazione della cibersicurezza»: una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC;

10) «sistema nazionale di certificazione della cibersicurezza»: una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, servizi TIC e processi TIC che rientrano nell'ambito di applicazione del sistema specifico;

11) «certificato europeo di cibersicurezza»: un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

12) «prodotto TIC»: un elemento o un gruppo di elementi di una rete o di un sistema informativo;

13) «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;

14) «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;

15) «accreditamento»: l'accreditamento quale definito all'articolo 2, punto 10), del regolamento (CE) n. 765/2008;

16) «organismo nazionale di accreditamento»: un organismo nazionale di accreditamento quale definito all'articolo 2, punto 11), del regolamento (CE) n. 765/2008;

17) «valutazione della conformità»: una valutazione della conformità ai sensi dell'articolo 2, punto 12), del regolamento (CE) n. 765/2008;

18) «organismo di valutazione della conformità»: un organismo di valutazione della conformità quale definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008;

19) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

20) «specifica tecnica»: un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC o un processo TIC deve soddisfare o le relative procedure di valutazione della conformità;

21) «livello di affidabilità»: base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC o processo TIC è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC o processo TIC interessato;

22) «autovalutazione di conformità»: un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC che valuta se tali prodotti TIC, servizi TIC e processi TIC soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersicurezza.

TITOLO II

ENISA — (AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA)

CAPO I

Mandato e obiettivi

Articolo 3

Mandato

1. L'ENISA svolge i compiti che le sono attribuiti ai sensi del presente regolamento allo scopo di conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersicurezza. L'ENISA funge da punto di riferimento per pareri e competenze in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione.

Svolgendo i compiti che le sono attribuiti ai sensi del presente regolamento, l'ENISA contribuisce a ridurre la frammentazione nel mercato interno.

2. L'ENISA svolge i compiti che le sono attribuiti dagli atti giuridici dell'Unione che stabiliscono le misure per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza.

3. Nello svolgimento dei suoi compiti, l'ENISA agisce in maniera indipendente, evitando nel contempo la duplicazione delle attività degli Stati membri e tenendo conto delle competenze esistenti degli Stati membri.

4. L'ENISA sviluppa le proprie risorse, incluse le capacità e abilità tecniche e umane, necessarie al fine di svolgere i compiti attribuitile ai sensi del presente regolamento.

Articolo 4

Obiettivi

1. L'ENISA opera come centro di competenze nel campo della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite, alle informazioni che mette a disposizione, alla trasparenza delle procedure, ai metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.

2. L'ENISA assiste le istituzioni, gli organi e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cibersicurezza, ivi comprese le politiche settoriali in materia di cibersicurezza.

3. L'ENISA sostiene lo sviluppo delle capacità e la preparazione nell'Unione, assistendo le istituzioni, gli organi e gli organismi dell'Unione, nonché gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersicurezza.

4. L'ENISA promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza.

5. L'ENISA contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.

6. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno. L'ENISA contribuisce all'istituzione e al mantenimento di un apposito quadro europeo di certificazione della cibersicurezza, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.

7. L'ENISA promuove un elevato livello di consapevolezza in materia di cibersicurezza, incluse l'igiene informatica e l'alfabetizzazione informatica, tra cittadini, organizzazioni e imprese.

CAPO II

Compiti

Articolo 5

Sviluppo e attuazione delle politiche e della normativa dell'Unione

L'ENISA contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione:

1) prestando assistenza e consulenza per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel campo della cibersicurezza e delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cibersicurezza, in particolare fornendo un parere indipendente, analisi nonché svolgendo lavori preparatori;

2) assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche emanando pareri e orientamenti, fornendo consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

3) assistendo gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nello sviluppo e nella promozione di politiche sulla cibersicurezza che sostengano la disponibilità generale o l'integrità del carattere fondamentale pubblico di una rete Internet aperta;

4) contribuendo ai lavori del gruppo di cooperazione di cui all'articolo 11 della direttiva (UE) 2016/1148, mettendo a disposizione le proprie competenze e fornendo assistenza;

5) sostenendo:

   a) lo sviluppo e l'attuazione della politica dell'Unione nel settore dell'identificazione elettronica e dei servizi fiduciari, in particolare fornendo consulenza e emanando orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti,

   b) la promozione di un livello di sicurezza più elevato delle comunicazioni elettroniche, anche fornendo consulenza e competenze e agevolando lo scambio delle migliori pratiche tra le autorità competenti,

   c) gli Stati membri nell'attuazione di aspetti specifici relativi alla cibersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e vita privata, anche fornendo su richiesta un parere al comitato europeo per la protezione dei dati;

6) sostenendo il riesame periodico delle attività politiche dell'Unione con la preparazione di una relazione annuale sullo stato di attuazione del relativo quadro giuridico per quanto riguarda:

   a) le informazioni sulle notifiche degli incidenti degli Stati membri trasmesse dal punto di contatto unico al gruppo di cooperazione, a norma dell'articolo 10, paragrafo 3, della direttiva (UE) 2016/1148,

   b) le sintesi delle notifiche di violazioni della sicurezza o perdita di integrità ricevute dai prestatori di servizi fiduciari trasmesse dagli organismi di vigilanza all'ENISA, a norma dell'articolo 19, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([23]);

   c) le notifiche relative a incidenti di sicurezza trasmesse dai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, trasmesse dalle autorità competenti all'ENISA, a norma dell'articolo 40 della direttiva (UE) 2018/1972.

([23]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

Articolo 6

Sviluppo delle capacità

1. L'ENISA assiste:

a) gli Stati membri nell'impegno a migliorare la prevenzione, la rilevazione e l'analisi delle minacce informatiche e degli incidenti, come pure la capacità di reazione agli stessi, fornendo loro le conoscenze e le competenze necessarie;

b) gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nella definizione e attuazione di politiche di divulgazione delle vulnerabilità su base volontaria;

c) le istituzioni, gli organi e gli organismi dell'Unione nel loro impegno a migliorare la prevenzione, la rilevazione e l'analisi delle minacce informatiche e degli incidenti, come pure a migliorare le loro capacità di reazione a tali minacce e incidenti, in particolare tramite un sostegno adeguato alla CERT-UE;

d) gli Stati membri nello sviluppo di CSIRT nazionali, ove richiesto a norma dell'articolo 9, paragrafo 5, della direttiva (UE) 2016/1148;

e) gli Stati membri nello sviluppo di strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, ove richiesto a norma dell'articolo 7, paragrafo 2, della direttiva (UE) 2016/1148, e promuove la diffusione di tali strategie in tutta l'Unione e prende nota del progresso della loro attuazione allo scopo di promuovere le migliori pratiche;

f) le istituzioni dell'Unione nello sviluppo e nella revisione di strategie dell'Unione in materia di cibersicurezza, nella promozione della loro diffusione e nel monitoraggio dei progressi compiuti nella loro attuazione;

g) i CSIRT nazionali e dell'Unione nell'innalzare il livello delle loro capacità, anche attraverso la promozione del dialogo e degli scambi di informazioni, al fine di assicurare che, tenuto conto dello stato dell'arte, tutti i CSIRT possiedano una serie comune di capacità minime e operino secondo le migliori pratiche;

h) gli Stati membri, mediante la periodica organizzazione di esercitazioni di cibersicurezza a livello di Unione di cui all'articolo 7, paragrafo 5, almeno ogni due anni e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

i) i pertinenti enti pubblici, attraverso l'offerta di formazione sulla cibersicurezza, se del caso in cooperazione con i portatori di interessi;

j) il gruppo di cooperazione, nello scambio di migliori pratiche, in particolare per quanto riguarda l'identificazione degli operatori di servizi essenziali da parte degli Stati membri, a norma dell'articolo 11, paragrafo 3, lettera l), della direttiva (UE) 2016/1148, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

2. L'ENISA sostiene la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulle procedure da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Articolo 7

Cooperazione operativa a livello di Unione

1. L'ENISA sostiene la cooperazione operativa tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e tra i portatori di interessi.

2. L'ENISA coopera a livello operativo e stabilisce sinergie con le istituzioni, gli organi e gli organismi dell'Unione, compresa la CERT-UE, con i servizi che si occupano della criminalità informatica e con le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di affrontare questioni di interesse comune, anche:

a) scambiando conoscenze e migliori pratiche;

b) fornendo consulenza ed emanando orientamenti sulle questioni pertinenti relative alla cibersicurezza;

c) stabilendo le disposizioni pratiche per l'esecuzione di compiti specifici, previa consultazione della Commissione.

3. L'ENISA svolge le funzioni di segretariato della rete di CSIRT, a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2016/1148, e in tale veste sostiene attivamente la condivisione delle informazioni e la cooperazione tra i suoi membri.

4. L'ENISA sostiene gli Stati membri nella cooperazione operativa nell'ambito della rete di CSIRT, mediante:

a) consigli su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi e, su richiesta di uno o più Stati membri, consigli in relazione a una specifica minaccia informatica;

b) l'assistenza, su richiesta di uno o più Stati membri, nella valutazione di incidenti aventi un impatto rilevante o sostanziale, tramite la messa a disposizione di competenze e l'agevolazione della gestione tecnica di tali incidenti, ivi compreso in particolare il sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri;

c) l'analisi delle vulnerabilità e degli incidenti sulla base delle informazioni pubblicamente disponibili o delle informazioni fornite volontariamente dagli Stati membri a tale scopo; e

d) su richiesta di uno o più Stati membri, il sostegno in relazione a indagini tecniche ex post sugli incidenti aventi un impatto rilevante o sostanziale ai sensi della direttiva (UE) 2016/1148.

Nello svolgimento di questi compiti, l'ENISA e la CERT-UE intraprendono una cooperazione strutturata per beneficiare delle sinergie ed evitare la duplicazione delle attività.

5. L'ENISA organizza periodicamente esercitazioni di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nell'organizzazione di esercitazioni di cibersicurezza. Tali esercitazioni di cibersicurezza a livello di Unione possono includere elementi tecnici, operativi o strategici. Ogni due anni l'ENISA organizza un'esercitazione globale su vasta scala.

Ove opportuno, l'ENISA inoltre contribuisce e aiuta ad organizzare esercitazioni di cibersicurezza settoriali insieme alle organizzazioni pertinenti che partecipano anche alle esercitazioni di cibersicurezza a livello di Unione.

6. L'ENISA elabora periodicamente, in stretta cooperazione con gli Stati membri, una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatiche, sulla base di informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro, dai CSIRT degli Stati membri o dai punti di contatto unici istituiti dalla direttiva (UE) 2016/1148, in entrambi i casi su base volontaria, dall'EC3 e dalla CERT-UE.

7. L'ENISA contribuisce a sviluppare una risposta cooperativa, a livello di Unione e di Stati membri, agli incidenti o alle crisi su vasta scala di carattere transfrontaliero connessi alla cibersicurezza, soprattutto:

a) aggregando e analizzando le relazioni delle fonti nazionali di dominio pubblico o condivise su base volontaria al fine di contribuire a creare una consapevolezza comune della situazione;

b) assicurando un flusso di informazioni efficiente e la disponibilità di meccanismi di attivazione tra la rete di CSIRT e i responsabili delle decisioni politiche e tecniche a livello di Unione;

c) agevolando, su richiesta, la gestione tecnica di tali incidenti o crisi, anche, in particolare, sostenendo la condivisione volontaria di soluzioni tecniche tra gli Stati membri;

d) sostenendo le istituzioni, gli organi e gli organismi dell'Unione e, su richiesta, gli Stati membri nella comunicazione pubblica in merito a tali incidenti o crisi;

e) verificando i piani di cooperazione per rispondere a tali incidenti o crisi a livello di Unione e sostenendo gli Stati membri, su loro richiesta, nella verifica di tali piani a livello nazionale.

Articolo 8

Mercato, certificazione della cibersicurezza e normazione

1. L'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC, come stabilito al titolo III del presente regolamento:

a) monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza secondo l'articolo 54, paragrafo 1, lettera c), in assenza di norme;

b) preparando proposte di sistemi europei di certificazione della cibersicurezza («proposte di sistemi») per prodotti TIC, servizi TIC e processi TIC conformemente all'articolo 49;

c) valutando i sistemi europei di certificazione della cibersicurezza adottati, conformemente all'articolo 49, paragrafo 8;

d) partecipando a valutazioni inter pares a norma dell'articolo 59, paragrafo 4;

e) assistendo la Commissione nel provvedere alle funzioni di segretariato dell'ECCG a norma dell'articolo 62, paragrafo 5.

2. L'ENISA provvede alle funzioni di segretariato del gruppo dei portatori di interessi per la certificazione della cibersicurezza a norma dell'articolo 22, paragrafo 4.

3. L'ENISA elabora e pubblica orientamenti e sviluppa buone pratiche in merito ai requisiti di cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC, in cooperazione con le autorità nazionali di certificazione della cibersicurezza e con il settore in modo formale, strutturato e trasparente.

4. L'ENISA contribuisce a uno sviluppo delle capacità relative ai processi di valutazione e certificazione mediante l'elaborazione e la pubblicazione di orientamenti, nonché fornendo sostegno agli Stati membri, su loro richiesta.

5. L'ENISA facilita la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC.

6. L'ENISA redige, in collaborazione con gli Stati membri e con il settore, pareri e orientamenti riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali, nonché riguardanti le norme già esistenti, comprese le norme nazionali degli Stati membri, ai sensi dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148.

7. L'ENISA effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante sia della domanda che dell'offerta, al fine di promuovere tale mercato nell'Unione.

Articolo 9

Conoscenze e informazioni

L'ENISA:

a) esegue analisi delle tecnologie emergenti e fornisce valutazioni su temi specifici in relazione agli impatti previsti, dal punto di vista sociale, giuridico, economico e regolamentare, delle innovazioni tecnologiche sulla cibersicurezza;

b) effettua analisi strategiche a lungo termine delle minacce informatiche e degli incidenti al fine di individuare le tendenze emergenti e contribuire a prevenire gli incidenti;

c) fornisce, in cooperazione con esperti delle autorità degli Stati membri e con i pertinenti portatori di interessi, consulenza, orientamenti e migliori pratiche per la sicurezza della rete e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148 e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva;

d) raggruppa, organizza e mette a disposizione del pubblico, tramite un portale dedicato, informazioni sulla cibersicurezza fornite dalle istituzioni, dagli organi e dagli organismi dell'Unione e informazioni sulla cibersicurezza fornite su base volontaria dagli Stati membri e dai portatori di interessi del settore pubblico e privato;

e) raccoglie e analizza le informazioni pubblicamente disponibili sugli incidenti di rilievo e redige relazioni al fine di fornire orientamenti ai cittadini, alle organizzazioni e alle imprese in tutta l'Unione.

Articolo 10

Sensibilizzazione e istruzione

L'ENISA:

a) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini, organizzazioni e imprese, anche per quanto concerne l'igiene informatica e l'alfabetizzazione informatica;

b) organizza regolarmente, in collaborazione con gli Stati membri, con le istituzioni, gli organi e gli organismi dell'Unione e con il settore, campagne di sensibilizzazione al fine di rafforzare la cibersicurezza e la sua visibilità nell'Unione e incoraggiare un ampio dibattito pubblico;

c) assiste gli Stati membri nei loro sforzi di sensibilizzazione e promuove l'istruzione in materia di cibersicurezza;

d) incoraggia un miglior coordinamento e scambio di migliori pratiche tra gli Stati membri per la sensibilizzazione e l'istruzione in materia di cibersicurezza.

Articolo 11

Ricerca e innovazione

Per quanto riguarda la ricerca e l'innovazione, l'ENISA:

a) fornisce consulenza alle istituzioni, agli organi e agli organismi dell'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel campo della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce informatiche attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

b) partecipa, qualora la Commissione gliene abbia delegato i poteri, alla fase di attuazione dei programmi di finanziamento per la ricerca e l'innovazione o in qualità di beneficiario;

c) contribuisce all'agenda strategica di ricerca e innovazione a livello dell'Unione nel campo della cibersicurezza.

Articolo 12

Cooperazione internazionale

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

a) impegnandosi, ove opportuno, in qualità di osservatore e nell'organizzazione delle esercitazioni internazionali, nonché analizzando i risultati di tali esercitazioni e comunicandoli al consiglio di amministrazione;

b) agevolando, su richiesta della Commissione, lo scambio di migliori pratiche;

c) fornendo competenze specialistiche alla Commissione, su richiesta della stessa;

d) fornendo consulenza e assistenza alla Commissione su questioni concernenti gli accordi con i paesi terzi per il riconoscimento reciproco dei certificati di cibersicurezza, in collaborazione con l'ECCG istituito a norma dell'articolo 62.

CAPO III

Organizzazione dell'ENISA

Articolo 13

Struttura dell'ENISA

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

a) un consiglio di amministrazione;

b) un comitato esecutivo;

c) un direttore esecutivo;

d) un gruppo consultivo ENISA;

e) una rete di funzionari nazionali di collegamento.

Section 1

Consiglio di amministrazione

Articolo 14

Composizione del consiglio di amministrazione

1. Il consiglio di amministrazione è composto da un membro nominato da ciascuno Stato membro e due membri nominati dalla Commissione. Tutti i membri hanno diritto di voto.

2. Ciascun membro del consiglio di amministrazione ha un supplente. Il supplente rappresenta il membro assente.

3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle loro pertinenti abilità gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza di genere equilibrata nel consiglio di amministrazione.

4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di quattro anni. Il mandato è rinnovabile.

Articolo 15

Funzioni del consiglio di amministrazione

1. Il consiglio di amministrazione:

a) stabilisce gli orientamenti generali del funzionamento dell'ENISA e assicura che operi secondo le regole e i principi stabiliti dal presente regolamento; assicura inoltre la coerenza del lavoro dell'ENISA con le attività svolte dagli Stati membri e a livello di Unione;

b) adotta il progetto di documento unico di programmazione dell'ENISA di cui all'articolo 24 prima che sia trasmesso alla Commissione per parere;

c) adotta il documento unico di programmazione dell'ENISA, tenendo conto del parere della Commissione;

d) vigila sull'attuazione della programmazione annuale e pluriennale contenuta nel documento unico di programmazione;

e) adotta il bilancio annuale dell'ENISA ed esercita altre funzioni in relazione al bilancio dell'ENISA a norma del capo IV;

f) valuta e adotta la relazione annuale consolidata sulle attività dell'ENISA, inclusi i conti e una descrizione di come l'ENISA ha conseguito i propri indicatori di risultato, trasmette, entro il 1º luglio dell'anno successivo, sia la relazione annuale che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti, e rende pubblica la relazione annuale;

g) adotta la regolamentazione finanziaria applicabile all'ENISA in conformità dell'articolo 32;

h) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;

i) adotta regole per la prevenzione e la gestione dei conflitti di interesse in relazione ai suoi membri;

j) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalle relazioni di revisione contabile e valutazioni interne o esterne;

k) adotta il proprio regolamento interno, comprese regole per le decisioni provvisorie sulla delega di compiti specifici, a norma dell'articolo 19, paragrafo 7;

l) esercita, nei confronti del personale dell'ENISA, i poteri conferiti dallo statuto dei funzionari («statuto dei funzionari») e dal regime applicabile agli altri agenti dell'Unione europea («regime applicabile agli altri agenti»), stabiliti nel regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([24]) all'autorità che ha il potere di nomina e all'autorità abilitata a concludere i contratti di assunzione («poteri dell'autorità che ha il potere di nomina») a norma del paragrafo 2 del presente articolo;

m) adotta le disposizioni di esecuzione dello statuto dei funzionari e del regime applicabile agli altri agenti secondo la procedura di cui all'articolo 110 dello statuto dei funzionari;

n) nomina il direttore esecutivo e, se del caso, ne proroga il mandato o lo rimuove dall'incarico, a norma dell'articolo 36;

o) nomina un contabile, che può essere il contabile della Commissione, che opera in piena indipendenza nell'esercizio delle sue funzioni;

p) prende tutte le decisioni sull'istituzione delle strutture interne dell'ENISA e, se necessario, sulla relativa modifica, in considerazione delle necessità per l'attività dell'ENISA e secondo una gestione di bilancio sana;

q) autorizza l'istituzione di accordi di lavoro in relazione all'articolo 7;

r) autorizza l'istituzione o la conclusione di accordi di lavoro conformemente all'articolo 42.

2. In conformità dell'articolo 110 dello statuto dei funzionari, il consiglio di amministrazione adotta una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i poteri di autorità che ha il potere di nomina e stabilisce le condizioni di sospensione della delega di poteri. Il direttore esecutivo può subdelegare tali poteri.

([24]) GU L 56 del 4.3.1968, pag. 1.

3. Qualora circostanze eccezionali lo richiedano, il consiglio di amministrazione può adottare una decisione per sospendere temporaneamente la delega al direttore esecutivo dei poteri di autorità che ha il potere di nomina e tutti i poteri di autorità che ha il potere di nomina che il direttore esecutivo abbia subdelegato ed esercitarli esso stesso o delegarli a uno dei suoi membri o a un membro del personale diverso dal direttore esecutivo.

Articolo 16

Presidente del consiglio di amministrazione

Il consiglio di amministrazione elegge tra i propri membri un presidente e un vicepresidente, a maggioranza dei due terzi dei membri. Il loro mandato è di quattro anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Articolo 17

Riunioni del consiglio di amministrazione

1. Il consiglio di amministrazione si riunisce su convocazione del suo presidente.

2. Il consiglio di amministrazione tiene almeno due riunioni ordinarie l'anno. Si riunisce inoltre in seduta straordinaria su richiesta del suo presidente, della Commissione o di almeno un terzo dei suoi membri.

3. Il direttore esecutivo partecipa alle riunioni del consiglio di amministrazione, ma non ha diritto di voto.

4. I membri del gruppo consultivo ENISA possono partecipare alle riunioni del consiglio di amministrazione su invito del presidente, ma non hanno diritto di voto.

5. Alle riunioni del consiglio di amministrazione, i membri del consiglio di amministrazione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno del consiglio di amministrazione.

6. L'ENISA provvede alle funzioni di segretariato del consiglio di amministrazione.

Articolo 18

Modalità di voto del consiglio di amministrazione

1. Il consiglio di amministrazione adotta le proprie decisioni a maggioranza dei suoi membri.

2. La maggioranza di due terzi dei membri del consiglio di amministrazione è necessaria per l'adozione del documento unico di programmazione e del bilancio annuale, nonché per la nomina del direttore esecutivo, la proroga del suo mandato o la sua rimozione dall'incarico.

3. Ogni membro dispone di un voto. In assenza di un membro, il supplente è abilitato a esercitare il diritto di voto del membro.

4. Il presidente del consiglio di amministrazione partecipa al voto.

5. Il direttore esecutivo non partecipa al voto.

6. Il regolamento interno del consiglio di amministrazione stabilisce le regole dettagliate concernenti la votazione, in particolare le circostanze in cui un membro può agire per conto di un altro.

Section 2

Comitato esecutivo

Articolo 19

Comitato esecutivo

1. Il consiglio di amministrazione è assistito da un comitato esecutivo.

2. Il comitato esecutivo:

a) prepara le decisioni che dovranno essere adottate dal consiglio di amministrazione;

b) insieme con il consiglio di amministrazione, garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'OLAF, nonché dalle relazioni di revisione contabile e valutazioni interne ed esterne;

c) fatte salve le responsabilità del direttore esecutivo stabilite all'articolo 20, fornisce assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione sulle questioni amministrative e di bilancio di cui all'articolo 20.

3. Il comitato esecutivo consta di cinque membri. I membri del comitato esecutivo sono nominati tra i membri del consiglio di amministrazione. Uno dei membri è il presidente del consiglio di amministrazione, che può anche presiedere il comitato esecutivo, e un altro è un rappresentante della Commissione. Le nomine dei membri del comitato esecutivo mirano ad assicurare l'equilibrio di genere nel comitato esecutivo. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.

4. La durata del mandato dei membri del comitato esecutivo è di quattro anni. Il mandato è rinnovabile.

5. Il comitato esecutivo si riunisce almeno una volta ogni tre mesi. Il presidente del comitato esecutivo convoca riunioni supplementari su richiesta dei suoi membri.

6. Il consiglio di amministrazione stabilisce il regolamento interno del comitato esecutivo.

7. Se necessario per ragioni di urgenza, il comitato esecutivo può prendere determinate decisioni provvisorie a nome del consiglio di amministrazione, in particolare su questioni di gestione amministrativa, tra cui la sospensione della delega dei poteri dell'autorità che ha il potere di nomina e le questioni di bilancio. Tali decisioni provvisorie sono notificate al consiglio di amministrazione senza indebiti ritardi. Il consiglio di amministrazione decide poi se approvare o rigettare la decisione provvisoria entro 3 mesi dalla sua adozione. Il comitato esecutivo non adotta per conto del consiglio di amministrazione decisioni richiedono l'approvazione di una maggioranza di due terzi dei membri del consiglio di amministrazione.

Section 3

Direttore esecutivo

Articolo 20

Funzioni del direttore esecutivo

1. L'ENISA è diretta dal suo direttore esecutivo, che è indipendente nell'esercizio delle sue funzioni. Il direttore esecutivo risponde al consiglio di amministrazione.

2. Su richiesta, il direttore esecutivo riferisce al Parlamento europeo sull'esercizio delle sue funzioni. Il Consiglio può invitare il direttore esecutivo a riferire sull'esercizio delle sue funzioni.

3. Il direttore esecutivo ha la responsabilità di:

a) provvedere all'amministrazione corrente dell'ENISA;

b) attuare le decisioni adottate dal consiglio di amministrazione;

c) preparare il documento unico di programmazione e presentarlo al consiglio di amministrazione per approvazione prima di trasmetterlo alla Commissione;

d) attuare il documento unico di programmazione e riferire in merito al consiglio di amministrazione;

e) elaborare la relazione annuale consolidata sulle attività dell'ENISA, compresa l'attuazione del suo programma di lavoro annuale, e presentarla al consiglio di amministrazione per valutazione e adozione;

f) predisporre un piano d'azione che dia seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti;

g) predisporre un piano d'azione che dia seguito alle conclusioni delle relazioni di revisione contabile interne ed esterne e delle indagini dell'OLAF e riferire due volte l'anno alla Commissione sui progressi compiuti e periodicamente al consiglio di amministrazione;

h) predisporre il progetto della regolamentazione finanziaria applicabile all'ENISA di cui all'articolo 32;

i) predisporre il progetto di stato di previsione delle entrate e delle spese dell'ENISA e l'esecuzione del bilancio;

j) proteggere gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, se del caso, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive;

k) elaborare una strategia antifrode dell'ENISA e presentarla al consiglio di amministrazione per approvazione;

l) sviluppare e mantenere i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con i portatori di interessi;

m) scambiare periodicamente opinioni e informazioni con le istituzioni, gli organi e gli organismi dell'Unione riguardo alle loro attività in materia di cibersicurezza, al fine di garantire la coerenza nello sviluppo e nell'attuazione delle politiche dell'Unione;

n) svolgere gli altri compiti attribuiti al direttore esecutivo dal presente regolamento.

4. In base alle esigenze e nell'ambito degli obiettivi e dei compiti dell'ENISA, il direttore esecutivo può istituire gruppi di lavoro ad hoc composti da esperti, anche esperti inviati dalle autorità competenti degli Stati membri. Il direttore esecutivo ne informa il consiglio di amministrazione in anticipo. Le procedure relative in particolare alla composizione dei gruppi di lavoro, alla nomina degli esperti dei gruppi di lavoro da parte del direttore esecutivo e al funzionamento dei gruppi di lavoro sono specificati nel regolamento interno dell'ENISA.

5. Se necessario, per svolgere i compiti dell'ENISA in maniera efficiente ed efficace e in base a un'adeguata analisi costi-benefici, il direttore esecutivo può decidere di istituire uno o più uffici locali in uno o più Stati membri. Prima di decidere di istituire un ufficio locale, il direttore esecutivo chiede il parere degli Stati membri interessati, compreso lo Stato membro che ospita la sede dell'ENISA, e ottiene il previo consenso della Commissione e del consiglio di amministrazione. In caso di disaccordo durante il processo di consultazione tra il direttore esecutivo e gli Stati membri interessati, la questione è sottoposta all'esame del Consiglio. Il numero complessivo dei membri del personale in tutti gli uffici locali è ridotto al minimo e non supera il 40 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede. Il numero dei membri del personale in ciascuno degli uffici locali non supera il 10 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede.

La decisione di istituire un ufficio locale precisa la gamma di attività che devono essere espletate presso l'ufficio locale al fine di evitare costi inutili e duplicazioni di funzioni amministrative dell'ENISA.

Section 4

Gruppo consultivo ENISA, gruppo dei portatori di interessi per la certificazione della cibersicurezza e rete dei funzionari nazionali di collegamento

Articolo 21

Gruppo consultivo ENISA

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce in maniera trasparente il gruppo consultivo ENISA, composto da esperti riconosciuti che rappresentano i pertinenti portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le PMI, gli operatori di servizi essenziali, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati in conformità della direttiva (UE) 2018/1972, delle organizzazioni europee di normazione nonché delle autorità di contrasto e delle autorità di controllo preposte alla protezione dei dati. Il consiglio di amministrazione si adopera per garantire un opportuno equilibrio geografico e di genere, nonché un equilibrio tra i diversi gruppi di portatori di interessi.

2. Le procedure per il gruppo consultivo ENISA, in particolare per quanto riguarda la composizione, la proposta del direttore esecutivo di cui al paragrafo 1, il numero e la nomina dei membri e il funzionamento del gruppo consultivo ENISA, sono specificati nel regolamento interno dell'ENISA e resi pubblici.

3. Il gruppo consultivo ENISA è presieduto dal direttore esecutivo o da qualsiasi altra persona nominata dal direttore esecutivo caso per caso.

4. Il mandato dei membri del gruppo consultivo ENISA è di due anni e mezzo. I membri del consiglio di amministrazione non possono essere membri del gruppo consultivo ENISA. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare alle riunioni del gruppo consultivo ENISA e a partecipare alle sue attività. Possono essere invitati a partecipare alle riunioni del gruppo consultivo ENISA e alle sue attività i rappresentanti di altri organismi che siano considerati pertinenti dal direttore esecutivo e non siano membri di tale gruppo.

5. Il gruppo consultivo ENISA fornisce consulenza all'ENISA relativamente allo svolgimento dei suoi compiti, tranne per quanto concerne l'applicazione delle disposizioni del titolo III del presente regolamento. In particolare, esso consiglia il direttore esecutivo ai fini della stesura di una proposta relativa al programma di lavoro annuale dell'ENISA e della comunicazione con i relativi portatori di interessi sulle questioni inerenti al programma di lavoro annuale.

6. Il gruppo consultivo ENISA informa periodicamente il consiglio di amministrazione sulle sue attività.

Articolo 22

Gruppo dei portatori di interessi per la certificazione della cibersicurezza

1. È istituito il gruppo dei portatori di interessi per la certificazione della cibersicurezza.

2. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza è composto da membri selezionati tra esperti riconosciuti che rappresentano i pertinenti portatori di interessi. La Commissione, a seguito di un invito aperto e trasparente, seleziona su proposta dell'ENISA i membri del gruppo dei portatori di interessi per la certificazione della cibersicurezza garantendo un equilibrio tra i diversi gruppi di portatori di interessi, nonché un opportuno equilibrio geografico e di genere.

3. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza:

a) fornisce consulenza alla Commissione sulle questioni strategiche riguardanti il quadro europeo di certificazione della cibersicurezza;

b) su richiesta, fornisce consulenza all'ENISA su questioni generali e strategiche concernenti i compiti della stessa in materia di mercato, certificazione della cibersicurezza e normazione;

c) assiste la Commissione nell'elaborazione del programma di lavoro progressivo dell'Unione di cui all'articolo 47;

d) formula un parere sul programma di lavoro progressivo dell'Unione a norma dell'articolo 47, paragrafo 4; e,

e) in casi urgenti, fornisce consulenza alla Commissione e all'ECCG in merito alla necessità di sistemi di certificazione supplementari non inclusi nel programma di lavoro progressivo dell'Unione, come previsto dagli articoli 47 e 48.

4. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza è copresieduto dai rappresentanti della Commissione e dell'ENISA ed è quest'ultima ad assicurarne il segretariato.

Articolo 23

Rete dei funzionari nazionali di collegamento

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce una rete dei funzionari nazionali di collegamento composta da rappresentanti di tutti gli Stati membri («funzionari nazionali di collegamento»). Ciascuno Stato membro designa un rappresentante nella rete dei funzionari nazionali di collegamento. Le riunioni della rete dei funzionari nazionali di collegamento possono svolgersi in diverse formazioni di esperti.

2. In particolare, la rete dei funzionari nazionali di collegamento agevola lo scambio di informazioni tra l'ENISA e gli Stati membri e sostiene l'ENISA nella diffusione, in tutta l'Unione, delle attività, dei risultati e delle raccomandazioni che la riguardano alle pertinenti parti interessate.

3. I funzionari nazionali di collegamento fungono da punto di contatto a livello nazionale per agevolare la cooperazione tra l'ENISA e gli esperti nazionali nel contesto dell'attuazione del programma di lavoro annuale dell'ENISA.

4. Mentre i funzionari nazionali di collegamento cooperano strettamente con i rappresentanti del consiglio di amministrazione dei rispettivi Stati membri, la rete dei funzionari nazionali di collegamento in sé non duplica il lavoro del consiglio di amministrazione o di altri consessi dell'Unione.

5. Le funzioni e le procedure relative alla rete dei funzionari nazionali di collegamento sono specificate nel regolamento interno dell'ENISA e rese pubbliche.

Section 5

Funzionamento

Articolo 24

Documento unico di programmazione

1. L'ENISA opera in conformità di un documento unico di programmazione contenente la programmazione annuale e pluriennale, che include tutte le attività pianificate.

2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti dalla Commissione, predispone un progetto di documento unico di programmazione contenente la pianificazione annuale e pluriennale delle risorse finanziarie e umane corrispondenti, secondo quanto previsto all'articolo 32 del regolamento delegato (UE) n. 1271/2013 della Commissione ([25]).

3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1 e lo trasmette al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, unitamente a eventuali successive versioni aggiornate di tale documento.

4. Il documento unico di programmazione diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione ed è adeguato secondo necessità.

([25]) Regolamento delegato (UE) n. 1271/2013 della Commissione, del 30 settembre 2013, che stabilisce il regolamento finanziario quadro degli organismi di cui all'articolo 208 del regolamento (UE, Euratom) n. 966/2012 del Parlamento europeo e del Consiglio (GU L 328 del 7.12.2013, pag. 42).

5. Il programma di lavoro annuale comprende gli obiettivi dettagliati e i risultati attesi, compresi gli indicatori di risultato. Esso contiene inoltre una descrizione delle azioni da finanziare e un'indicazione delle risorse finanziarie e umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio per attività e gestione per attività. Il programma di lavoro annuale è coerente con il programma di lavoro pluriennale di cui al paragrafo 7. Indica chiaramente i compiti aggiunti, modificati o soppressi rispetto all'esercizio finanziario precedente.

6. Quando all'ENISA è assegnato un nuovo compito, il consiglio di amministrazione modifica il programma di lavoro annuale adottato. Le modifiche sostanziali del programma di lavoro annuale sono adottate con la stessa procedura di quella applicabile al programma di lavoro annuale iniziale. Il consiglio di amministrazione può delegare al direttore esecutivo il potere di apportare modifiche non sostanziali al programma di lavoro annuale.

7. Il programma di lavoro pluriennale definisce la programmazione strategica generale, compresi gli obiettivi, i risultati attesi e gli indicatori di prestazione. Riporta inoltre la programmazione delle risorse, compresi il bilancio pluriennale e il personale.

8. La programmazione delle risorse è aggiornata ogni anno. La programmazione strategica è aggiornata secondo necessità, in particolare per adattarla all'esito della valutazione di cui all'articolo 67.

Articolo 25

Dichiarazione di interessi

1. I membri del consiglio di amministrazione, il direttore esecutivo, come pure i funzionari distaccati dagli Stati membri a titolo temporaneo, rendono ciascuno una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza. Le dichiarazioni sono precise e complete, presentate ogni anno per iscritto e aggiornate ogniqualvolta sia necessario.

2. I membri del consiglio di amministrazione, il direttore esecutivo e gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano ciascuno in modo preciso e completo, al più tardi all'inizio di ogni riunione, qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del giorno e si astengono dal partecipare alle discussioni e alle votazioni inerenti tali punti.

3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per le regole sulle dichiarazioni di interessi di cui ai paragrafi 1 e 2.

Articolo 26

Trasparenza

1. L'ENISA svolge le proprie attività con un livello elevato di trasparenza e nel rispetto dell'articolo 28.

2. L'ENISA provvede a che al pubblico e alle parti interessate siano fornite informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 25.

3. Il consiglio di amministrazione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività dell'ENISA.

4. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2.

Articolo 27

Riservatezza

1. Fatto salvo l'articolo 28, l'ENISA non rivela a terzi le informazioni da essa trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato.

2. I membri del consiglio di amministrazione, il direttore esecutivo, i membri del gruppo consultivo ENISA, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'ENISA, compresi i funzionari distaccati dagli Stati membri a titolo temporaneo, rispettano gli obblighi di riservatezza dell'articolo 339 TFUE anche dopo la cessazione delle proprie funzioni.

3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di riservatezza di cui ai paragrafi 1 e 2.

4. Se necessario ai fini dell'esecuzione dei compiti dell'ENISA, il consiglio di amministrazione decide di consentire all'ENISA di trattare informazioni classificate. In questo caso, l'ENISA, in accordo con i servizi della Commissione, adotta regole in materia di sicurezza che applichino i principi di sicurezza enunciati nelle decisioni (UE, Euratom) 2015/443 ([26]) e 2015/444 ([27]) della Commissione. Tali regole in materia di sicurezza disciplinano, tra l'altro, lo scambio, il trattamento e la conservazione di informazioni classificate.

Articolo 28

Accesso ai documenti

1. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dall'ENISA.

2. Entro il 28 dicembre 2019, il consiglio di amministrazione adotta disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

3. Le decisioni adottate dall'ENISA a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono formare oggetto di una denuncia presentata al Mediatore europeo a norma dell'articolo 228 TFUE o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 TFUE.

CAPO IV

Formazione e struttura del bilancio dell'ENISA

Articolo 29

Formazione del bilancio dell'ENISA

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo e lo trasmette al consiglio di amministrazione, corredato di un progetto di tabella dell'organico. Le entrate e le spese devono risultare in pareggio.

2. Ogni anno il consiglio di amministrazione elabora, sulla base del progetto di stato di previsione, uno stato di previsione delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo.

3. Entro il 31 gennaio di ogni anno il consiglio di amministrazione invia lo stato di previsione, come parte integrante del progetto di documento unico di programmazione, alla Commissione e ai paesi terzi con cui l'Unione ha concluso accordi di cui all'articolo 42, paragrafo 2.

4. Sulla base dello stato di previsione, la Commissione iscrive le stime che ritiene necessarie, per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale dell'Unione, nel progetto di bilancio generale dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente all'articolo 314 TFUE.

5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo dell'Unione all'ENISA.

6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico dell'ENISA.

([26]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

([27]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

7. Insieme al documento unico di programmazione, il consiglio di amministrazione adotta il bilancio dell'ENISA. Il bilancio dell'ENISA diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Ove necessario, il consiglio di amministrazione modifica il bilancio e il documento unico di programmazione dell'ENISA per conformarli al bilancio generale dell'Unione.

Articolo 30

Struttura del bilancio dell'ENISA

1. Fatte salve altre risorse, le entrate dell'ENISA comprendono:

a) un contributo dal bilancio generale dell'Unione;

b) entrate con destinazione specifica volte a finanziare spese specifiche conformemente alla regolamentazione finanziaria di cui all'articolo 32;

c) finanziamenti dell'Unione sotto forma di accordi di delega o di sovvenzioni ad hoc secondo la regolamentazione finanziaria di cui all'articolo 32 e le disposizioni dei pertinenti strumenti di sostegno alle politiche dell'Unione;

d) contributi dei paesi terzi che partecipano ai lavori dell'ENISA di cui all'articolo 42;

e) eventuali contributi volontari degli Stati membri, in denaro o in natura.

Gli Stati membri che versano contributi volontari ai sensi del primo comma, lettera e), non possono rivendicare alcun diritto o servizio specifico per effetto di tale contributo.

2. Le spese dell'ENISA comprendono la retribuzione del personale, l'assistenza amministrativa e tecnica, le spese infrastrutturali e di esercizio, nonché quelle conseguenti a contratti con terzi.

Articolo 31

Esecuzione del bilancio dell'ENISA

1. Il direttore esecutivo è responsabile dell'esecuzione del bilancio dell'ENISA.

2. Il revisore contabile interno della Commissione esercita nei confronti dell'ENISA le stesse competenze di cui dispone nei confronti dei servizi della Commissione.

3. Il contabile dell'ENISA comunica i conti provvisori per l'esercizio (anno N) al contabile della Commissione e alla Corte dei conti entro il 1º marzo dell'esercizio successivo (anno N + 1).

4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti provvisori dell'ENISA a norma dell'articolo 246 del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio ([28]), il contabile dell'ENISA redige i conti definitivi dell'ENISA sotto la propria responsabilità e li presenta al consiglio di amministrazione per parere.

5. Il consiglio di amministrazione formula un parere sui conti definitivi dell'ENISA.

6. Entro il 31 marzo dell'anno N + 1, il direttore esecutivo trasmette la relazione sulla gestione di bilancio e finanziaria al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.

7. Entro il 1º luglio dell'anno N + 1, il contabile dell'ENISA trasmette i conti definitivi dell'ENISA, accompagnati dal parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, al contabile della Commissione e alla Corte dei conti.

([28]) 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).

8. Contemporaneamente ai conti definitivi dell'ENISA, il contabile dell'ENISA trasmette altresì alla Corte dei conti, e in copia al contabile della Commissione, una dichiarazione ad essi relativa.

9. Entro il 15 novembre dell'anno N + 1 il direttore esecutivo pubblica i conti definitivi dell'ENISA nella *Gazzetta ufficiale dell'Unione europea*.

10. Entro il 30 settembre dell'anno N + 1 il direttore esecutivo invia alla Corte dei conti una risposta alle osservazioni da essa formulate e ne trasmette copia al consiglio di amministrazione e alla Commissione.

11. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo, tutte le informazioni necessarie al corretto svolgimento della procedura di discarico per l'esercizio in causa, in conformità dell'articolo 261, paragrafo 3, del regolamento (UE, Euratom) 2018/1046.

12. Il Parlamento europeo, su raccomandazione del Consiglio, concede il discarico al direttore esecutivo, entro il 15 maggio dell'anno N + 2, per l'esecuzione del bilancio dell'esercizio N.

Articolo 32

Regolamentazione finanziaria

La regolamentazione finanziaria applicabile all'ENISA è adottata dal consiglio di amministrazione previa consultazione della Commissione. Essa si discosta dal regolamento delegato (UE) n. 1271/2013 solo per esigenze specifiche di funzionamento dell'ENISA e previo accordo della Commissione.

Articolo 33

Lotta antifrode

1. Per facilitare la lotta contro la frode, la corruzione e altre attività illecite ai sensi del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio ([29]), entro il 28 dicembre 2019 l'ENISA aderisce all'accordo interistituzionale del 25 maggio 1999 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo interne alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) ([30]). L'ENISA adotta opportune disposizioni valide per l'insieme dei propri dipendenti, utilizzando i modelli riportati nell'allegato di tale accordo.

2. La Corte dei conti ha potere di verifica, esercitabile su documenti e mediante ispezioni in loco, su tutti i beneficiari di sovvenzioni, i contraenti e i subcontraenti che hanno beneficiato di fondi dell'Unione da parte dell'ENISA.

3. L'OLAF può eseguire indagini, compresi controlli e verifiche sul posto, in conformità delle disposizioni e delle procedure stabilite dal regolamento (UE, Euratom) n. 883/2013 e dal regolamento (Euratom, CE) n. 2185/96 del Consiglio ([31]), per accertare casi di frode, corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dall'ENISA.

4. Fatti salvi i paragrafi 1, 2 e 3, gli accordi di cooperazione con paesi terzi o organizzazioni internazionali, i contratti, le convenzioni di sovvenzione e le decisioni di sovvenzione dell'ENISA contengono disposizioni che autorizzano esplicitamente la Corte dei conti e l'OLAF a procedere a tali revisioni contabili e indagini conformemente alle loro rispettive competenze.

([29]) Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

([30]) GU L 136 del 31.5.1999, pag. 15.

([31]) Regolamento (Euratom, CE) n 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2).

CAPO V

Personale

Articolo 34

Disposizioni generali

Al personale dell'ENISA si applicano lo statuto dei funzionari, il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per dare applicazione allo statuto dei funzionari e al regime applicabile agli altri agenti.

Articolo 35

Privilegi e immunità

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

Articolo 36

Direttore esecutivo

1. Il direttore esecutivo è assunto come agente temporaneo dell'ENISA ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.

2. Il direttore esecutivo è nominato dal consiglio di amministrazione in base a un elenco di candidati proposto dalla Commissione, secondo una procedura di selezione aperta e trasparente.

3. Ai fini della conclusione del contratto di lavoro del direttore esecutivo, l'ENISA è rappresentata dal presidente del consiglio di amministrazione.

4. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione è invitato a fare una dichiarazione dinanzi alla commissione competente del Parlamento europeo e a rispondere alle domande dei deputati.

5. La durata del mandato del direttore esecutivo è di cinque anni. Entro la fine di tale periodo, la Commissione esegue una valutazione della prestazione del direttore esecutivo e dei compiti e delle sfide futuri dell'ENISA.

6. Il consiglio di amministrazione adotta le decisioni riguardanti la nomina del direttore esecutivo, la proroga del suo mandato e la sua rimozione dall'incarico in conformità dell'articolo 18, paragrafo 2.

7. Su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di amministrazione può prorogare il mandato del direttore esecutivo una sola volta, per cinque anni.

8. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo. Entro i tre mesi che precedono tale proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.

9. Il direttore esecutivo il cui mandato sia stato prorogato non partecipa a un'altra procedura di selezione per lo stesso posto.

10. Il direttore esecutivo può essere rimosso dall'incarico solo su decisione del consiglio di amministrazione, su proposta della Commissione.

Articolo 37

Esperti nazionali distaccati e altro personale

1. L'ENISA può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze. Lo statuto dei funzionari e il regime applicabile agli altri agenti non si applicano a tale personale.

2. Il consiglio di amministrazione adotta una decisione che stabilisce le regole relative al distacco di esperti nazionali presso l'ENISA.

CAPO VI

Disposizioni generali relative all'ENISA

Articolo 38

Status giuridico dell'ENISA

1. L'ENISA è un organismo dell'Unione ed è dotata di personalità giuridica.

2. L'ENISA gode, in ciascuno Stato membro, della più ampia capacità giuridica riconosciuta alle persone giuridiche dal diritto nazionale. In particolare, può acquistare o alienare beni mobili e immobili e stare in giudizio.

3. L'ENISA è rappresentata dal direttore esecutivo.

Articolo 39

Responsabilità dell'ENISA

1. La responsabilità contrattuale dell'ENISA è disciplinata dal diritto applicabile al contratto.

2. La Corte di giustizia dell'Unione europea è competente a giudicare in virtù di clausole compromissorie contenute nel contratto concluso dall'ENISA.

3. In materia di responsabilità extracontrattuale, l'ENISA è obbligata al risarcimento dei danni cagionati da essa o dai membri del suo personale nell'esercizio delle loro funzioni, secondo i principi generali comuni agli ordinamenti degli Stati membri.

4. La Corte di giustizia dell'Unione europea è competente a conoscere delle controversie relative al risarcimento dei danni di cui al paragrafo 3.

5. La responsabilità personale del personale dell'ENISA nei confronti dell'ENISA è disciplinata dalle disposizioni pertinenti che si applicano al personale dell'ENISA.

Articolo 40

Regime linguistico

1. All'ENISA si applica il regolamento n. 1 del Consiglio ([32]). Gli Stati membri e gli altri organismi designati dagli Stati membri possono rivolgersi all'ENISA e ottenere la risposta in una delle lingue ufficiali delle istituzioni dell'Unione di loro scelta.

2. I servizi di traduzione necessari per il funzionamento dell'ENISA sono forniti dal Centro di traduzione degli organismi dell'Unione europea.

Articolo 41

Protezione dei dati personali

1. Il trattamento dei dati personali da parte dell'ENISA è soggetto al regolamento (UE) 2018/1725.

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

([32]) Regolamento del Consiglio n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU 17 del 6.10.1958, pag. 385).

Articolo 42

Cooperazione con paesi terzi e organizzazioni internazionali

1. Nella misura necessaria ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'ENISA può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'ENISA può istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali, previa approvazione da parte della Commissione. Detti accordi di lavoro non creano obblighi giuridici per l'Unione e gli Stati membri.

2. L'ENISA è aperta alla partecipazione di paesi terzi che abbiano concluso con l'Unione accordi in tal senso. Nell'ambito delle pertinenti disposizioni di tali accordi, sono istituiti accordi di lavoro che specificano, in particolare, la natura, la portata e le modalità di partecipazione di detti paesi terzi ai lavori dell'ENISA, e comprendono disposizioni sulla partecipazione alle iniziative intraprese dall'ENISA, sui contributi finanziari e sul personale. In materia di personale, tali accordi di lavoro rispettano in ogni caso lo statuto dei funzionari e il regime applicabile agli altri agenti.

3. Il consiglio di amministrazione adotta una strategia per le relazioni con paesi terzi e organizzazioni internazionali riguardo a questioni che rientrano tra le competenze dell'ENISA. La Commissione garantisce che l'ENISA operi nell'ambito del proprio mandato e del quadro istituzionale vigente stipulando accordi di lavoro adeguati con il direttore esecutivo.

Articolo 43

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

Previa consultazione della Commissione, l'ENISA adotta regole in materia di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni sensibili non classificate e delle ICUE di cui alle decisioni (UE, Euratom) 2015/443 e 2015/444. Le regole in materia di sicurezza dell'ENISA includono le disposizioni che disciplinano lo scambio, il trattamento e la conservazione di tali informazioni.

Articolo 44

Accordo sulla sede e condizioni operative

1. Le necessarie disposizioni relative all'insediamento dell'ENISA nello Stato membro ospitante e alle strutture che quest'ultimo deve mettere a disposizione nonché le regole specifiche applicabili in tale Stato membro al direttore esecutivo, ai membri del consiglio di amministrazione, al personale dell'ENISA e ai membri delle rispettive famiglie sono fissate in un accordo di sede concluso tra l'ENISA e lo Stato membro ospitante, previa approvazione del consiglio di amministrazione.

2. Lo Stato membro che ospita l'ENISA fornisce le migliori condizioni possibili volte a garantire il corretto funzionamento dell'ENISA, tenendo conto dell'accessibilità della sede, dell'esistenza di strutture scolastiche adeguate per i figli del personale, di un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi dei membri del personale.

Articolo 45

Controllo amministrativo

L'operato dell'ENISA è sottoposto al controllo del Mediatore europeo in conformità dell'articolo 228 TFUE.

TITOLO III

QUADRO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Articolo 46

Quadro europeo di certificazione della cibersicurezza

1. È istituito il quadro europeo di certificazione della cibersicurezza al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC.

2. Il quadro europeo di certificazione della cibersicurezza prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita.

Articolo 47

Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza

1. La Commissione pubblica un programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza («programma di lavoro progressivo dell'Unione») in cui sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza.

2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.

3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC e processi TIC o delle relative categorie è giustificata sulla base di una o più delle seguenti motivazioni:

a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC o processi TIC e in particolare in relazione al rischio di frammentazione;

b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri;

c) la domanda di mercato;

d) gli sviluppi nel panorama delle minacce informatiche;

e) la richiesta di preparazione di una specifica proposta di sistema da parte del'ECCG.

4. La Commissione tiene nella debita considerazione i pareri in merito al progetto di programma di lavoro progressivo dell'Unione espressi dall'ECCG e dal gruppo dei portatori di interessi per la certificazione della cibersicurezza.

5. Il primo programma di lavoro progressivo dell'Unione è pubblicato entro il 28 giugno 2020. Il programma di lavoro progressivo dell'Unione è aggiornato almeno ogni tre anni e più spesso se necessario.

Articolo 48

Richiesta di un sistema europeo di certificazione della cibersicurezza

1. La Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente sulla base del programma di lavoro progressivo dell'Unione.

2. In casi debitamente giustificati la Commissione o l'ECCG può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente non incluso nel programma di lavoro progressivo dell'Unione. Il programma di lavoro progressivo dell'Unione è aggiornato di conseguenza.

Articolo 49

Preparazione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza

1. A seguito di una richiesta della Commissione ai sensi dell'articolo 48, l'ENISA prepara una proposta di sistema che soddisfi i requisiti di cui agli articoli 51, 52 e 54.

2. A seguito di una richiesta dell'ECCG a norma dell'articolo 48, paragrafo 2, l'ENISA può preparare una proposta di sistema che soddisfi i requisiti di cui agli articoli 51, 52 e 54. Qualora respinga tale richiesta, l'ENISA motiva il proprio rifiuto. Ogni decisione di rifiuto della richiesta è presa dal consiglio di amministrazione.

3. Nella preparazione di una proposta di sistema, l'ENISA consulta tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo.

4. Per ciascuna proposta di sistema, l'ENISA istituisce un gruppo di lavoro ad hoc in conformità dell'articolo 20, paragrafo 4, con l'obiettivo di fornire all'ENISA consulenza e competenze specifiche.

5. L'ENISA coopera strettamente con l'ECCG. L'ECCG fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e adotta un parere sulla proposta.

6. L'ENISA tiene nella massima considerazione il parere dell'ECCG prima di trasmettere alla Commissione la proposta di sistema preparata in conformità dei paragrafi 3, 4 e 5. Il parere dell'ECCG non vincola l'ENISA e la sua assenza non impedisce all'ENISA di trasmettere la proposta di sistema alla Commissione.

7. La Commissione, sulla base della proposta di sistema preparata dall'ENISA, può adottare atti di esecuzione, prevedendo un sistema europeo di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC che soddisfano i requisiti di cui agli articoli 51, 52 e 54. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

8. Almeno ogni cinque anni l'ENISA valuta ogni sistema europeo di certificazione della cibersicurezza adottato, tenendo conto del riscontro ricevuto dalle parti interessate. Se necessario, la Commissione o l'ECCG può chiedere all'ENISA di avviare il processo di sviluppo di una proposta riveduta di sistema in conformità dell'articolo 48 e del presente articolo.

Articolo 50

Sito web sui sistemi europei di certificazione della cibersicurezza

1. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza, sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità, e li pubblicizza, comprese le informazioni sui certificati europei di cibersicurezza che non sono più validi, sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità revocati e scaduti e sul repertorio di link a informazioni sulla cibersicurezza fornite a norma dell'articolo 55.

2. Ove applicabile, il sito web di cui al paragrafo 1 indica inoltre i sistemi di certificazione della cibersicurezza nazionali che sono stati sostituiti da un sistema europeo di certificazione della cibersicurezza.

Articolo 51

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:

a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

c) le persone, i programmi o le macchine autorizzati devono poter accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

d) individuare e documentare le dipendenze e vulnerabilità note;

e) registrare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

f) fare in modo che si possa verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso, che sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

g) verificare che i prodotti TIC, i servizi TIC e i processi TIC non contengano vulnerabilità note;

h) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;

i) i prodotti TIC, i servizi TIC e i processi TIC devono essere sicuri fin dalla progettazione e per impostazione predefinita;

j) il software e l'hardware dei prodotti TIC, dei servizi TIC e dei processi TIC devono essere aggiornati, non contenere vulnerabilità pubblicamente note e devono disporre di meccanismi per effettuare aggiornamenti protetti.

Articolo 52

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC e i processi TIC uno o più dei seguenti livelli di affidabilità: «di base», «sostanziale» o «elevato». Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente.

2. I certificati europei di cibersicurezza e le dichiarazioni UE di conformità si riferiscono a qualsiasi livello di affidabilità specificato nel sistema europeo di certificazione della cibersicurezza nell'ambito del quale si rilascia il certificato europeo di cibersicurezza o la dichiarazione UE di conformità.

3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersicurezza pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti della valutazione a cui deve essere sottoposto il prodotto TIC, servizio TIC o processo TIC.

4. Il certificato o la dichiarazione UE di conformità si riferiscono a specifiche tecniche, norme e procedure ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli

5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità «di base» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

6. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «sostanziale» assicura che i prodotti TIC, servizi TIC e processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

7. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «elevato» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.

8. I sistemi europei di certificazione della cibersicurezza possono precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia di valutazione utilizzata. Ciascun livello di valutazione corrisponde a uno dei livelli di affidabilità ed è definito da un'idonea combinazione di componenti dell'affidabilità.

Articolo 53

Autovalutazione della conformità

1. Un sistema europeo di certificazione della cibersicurezza può consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC o processi TIC. Tale autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, servizi TIC e processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità «di base».

2. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC si assume la responsabilità della conformità del prodotto TIC, servizio TIC o processo TIC ai requisiti previsti in tale sistema.

3. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC rende disponibile all'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema. Una copia della dichiarazione UE di conformità è trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

4. Il rilascio di una dichiarazione UE di conformità è volontario, salvo diversamente specificato nel diritto dell'Unione o degli Stati membri.

5. Le dichiarazioni UE di conformità sono riconosciute in tutti gli Stati membri.

Articolo 54

Elementi dei sistemi europei di certificazione della cibersicurezza

1. Un sistema europeo di certificazione della cibersicurezza comprende almeno i seguenti elementi:

a) l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo o le categorie di prodotti TIC, servizi TIC o processi TIC coperti;

b) una chiara descrizione dello scopo del sistema e delle modalità con cui le norme, i metodi di valutazione e i livelli di affidabilità selezionati corrispondono alle esigenze degli utenti del sistema previsti;

c) i riferimenti alle norme internazionali, europee o nazionali applicate nella valutazione o, laddove tali norme non siano disponibili o adeguate, alle specifiche tecniche che rispettano le prescrizioni enunciate all'allegato II del regolamento (UE) n. 1025/2012 oppure, se tali specifiche non sono disponibili, alle specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema europeo di certificazione della cibersicurezza;

d) se del caso, uno o più livelli di affidabilità;

e) l'indicazione se l'autovalutazione della conformità sia autorizzata nell'ambito del sistema;

f) se del caso, requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cibersicurezza;

g) i criteri e i metodi di valutazione specifici da utilizzare, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi di sicurezza di cui all'articolo 51 sono stati conseguiti;

h) se del caso, le informazioni che sono necessarie per la certificazione e che un richiedente deve fornire agli organismi di valutazione della conformità o che deve altrimenti mettere a loro disposizione;

i) le condizioni alle quali possono essere utilizzati gli eventuali marchi o etichette previsti dal sistema;

j) le regole per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC ai requisiti dei certificati europei di cibersicurezza o delle dichiarazioni UE di conformità, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;

k) se del caso, le condizioni per il rilascio, il mantenimento, la prosecuzione e il rinnovo dei certificati europei di cibersicurezza, nonché le condizioni per l'estensione o la riduzione del campo di applicazione della certificazione;

l) le regole riguardanti le conseguenze per i prodotti TIC, servizi TIC e processi TIC che sono stati certificati o per i quali è stata rilasciata una dichiarazione UE di conformità ma che non sono conformi ai requisiti del sistema;

m) le regole riguardanti il modo in cui segnalare e trattare le vulnerabilità della cibersicurezza nei prodotti TIC, servizi TIC e processi TIC precedentemente non rilevate;

n) se del caso, le regole riguardanti la conservazione dei registri da parte degli organismi di valutazione della conformità;

o) l'individuazione dei sistemi nazionali o internazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti TIC, servizi TIC e processi TIC, requisiti di sicurezza, criteri e metodi di valutazione nonché livelli di affidabilità;

p) il contenuto e il formato dei certificati europei di cibersicurezza e le dichiarazioni UE di conformità da rilasciare;

q) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti da rendere disponibili da parte del fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC;

r) il periodo massimo di validità dei certificati europei di cibersicurezza rilasciati nell'ambito del sistema;

s) la politica di divulgazione dei certificati europei di cibersicurezza rilasciati, modificati o revocati nell'ambito del sistema;

t) le condizioni per il riconoscimento reciproco dei sistemi di certificazione con i paesi terzi;

u) se del caso, le regole riguardanti eventuali meccanismi di valutazione inter pares istituito dal sistema per le autorità o gli organismi che rilasciano certificati europei di cibersicurezza per il livello di affidabilità «elevato» a norma dell'articolo 56, paragrafo 6. Tali meccanismi non pregiudicano la valutazione inter pares di cui all'articolo 59;

v) il formato e le procedure che i fabbricanti o i fornitori di prodotti TIC, servizi TIC o processi TIC devono rispettare nel fornire e aggiornare le informazioni supplementari sulla cibersicurezza a norma dell'articolo 55.

2. I requisiti specificati del sistema europeo di certificazione della cibersicurezza devono essere coerenti con gli obblighi di legge applicabili, in particolare quelli derivanti dal diritto armonizzato dell'Unione.

3. Se un atto giuridico specifico dell'Unione lo prevede, un certificato o una dichiarazione UE di conformità rilasciati nell'ambito di un sistema europeo di certificazione della cibersicurezza possono essere utilizzati per dimostrare la presunzione di conformità agli obblighi imposti da tale atto giuridico.

4. In assenza di diritto armonizzato dell'Unione, anche il diritto degli Stati membri può disporre che un sistema europeo di certificazione della cibersicurezza possa essere utilizzato per stabilire la presunzione di conformità agli obblighi di legge.

Articolo 55

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

1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC certificati o prodotti TIC, servizi TIC o processi per i quali è stata rilasciata una dichiarazione UE di conformità rende pubblicamente disponibili le seguenti informazioni supplementari sulla cibersicurezza:

a) orientamenti e raccomandazioni che assistano gli utenti finali nel configurare, installare, avviare, operare e mantenere in modo sicuro i prodotti TIC o servizi TIC;

b) il periodo durante il quale agli utenti finali sarà offerta assistenza di sicurezza, in particolare per quanto concerne la disponibilità di aggiornamenti connessi alla cibersicurezza;

c) informazioni di contatto del fabbricante o fornitore e metodi accettati per ricevere informazioni sulle vulnerabilità dagli utenti finali e dai ricercatori nel settore della sicurezza;

d) un riferimento ad archivi online in cui siano elencate le vulnerabilità comunicate al pubblico relative al prodotto TIC, servizio TIC o processo TIC e a tutti i relativi consigli in materia di cibersicurezza.

2. Le informazioni di cui al paragrafo 1 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, almeno fino alla scadenza del certificato europeo di cibersicurezza o della dichiarazione UE di conformità corrispondenti.

Articolo 56

Certificazione della cibersicurezza

1. I prodotti TIC, i servizi TIC e i processi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 sono considerati conformi ai requisiti di tale sistema.

2. La certificazione della cibersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o degli Stati membri.

3. La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e migliorare il funzionamento del mercato interno. La prima valutazione di questo genere è effettuata entro il 31 dicembre 2023 e le successive valutazioni sono effettuate almeno ogni due anni. Sulla base dei risultati di tali valutazioni, la Commissione individua i prodotti TIC, servizi TIC e processi TIC coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione.

In via prioritaria la Commissione si concentra sui settori elencati all'allegato II della direttiva (UE) 2016/1148, che sono sottoposti a valutazione al più tardi due anni dopo l'adozione del primo sistema europeo di certificazione della cibersicurezza.

Nel preparare la valutazione la Commissione:

a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC o processi TIC e sugli utenti in termini di costi di tali misure nonché i benefici sociali o economici derivanti dal previsto aumento del livello di sicurezza per i prodotti TIC, i servizi TIC o i processi TIC in questione;

b) tiene conto dell'esistenza e dell'attuazione di diritto degli Stati membri e dei paesi terzi in materia;

c) procede a un processo di consultazione aperto, trasparente e inclusivo con tutti i pertinenti portatori di interesse e gli Stati membri;

d) prende in considerazione le scadenze di attuazione e le misure transitorie e i periodi di transizione, in particolare con riferimento al possibile impatto delle misure sui fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC, PMI comprese;

e) propone il modo più rapido ed efficace per realizzare la transizione da un sistema di certificazione volontario a uno obbligatorio.

4. Gli organismi di valutazione della conformità di cui all'articolo 60 rilasciano certificati europei di cibersicurezza ai sensi del presente articolo che fanno riferimento a un livello di affidabilità «di base» o «sostanziale» sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza adottato dalla Commissione a norma dell'articolo 49.

5. In deroga al paragrafo 4, in casi debitamente giustificati un sistema europeo di certificazione della cibersicurezza può prevedere che i certificati europei di cibersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico. Detto ente è uno dei seguenti:

a) un'autorità nazionale di certificazione della cibersicurezza ai sensi dell'articolo 58, paragrafo 1; o

b) un organismo pubblico accreditato come organismo di valutazione della conformità a norma dell'articolo 60, paragrafo 1.

6. Ove un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 richieda un livello di affidabilità «elevato», il certificato europeo di cibersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza oppure, nei casi seguenti, da un organismo di valutazione della conformità:

a) previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità; o

b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cibersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

7. La persona fisica o giuridica che presenta i prodotti TIC, servizi TIC o processi TIC per la certificazione mette a disposizione dell'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersicurezza, o dell'organismo di valutazione della conformità di cui all'articolo 60 tutte le informazioni necessarie a espletare la certificazione.

8. Il titolare di un certificato europeo di cibersicurezza informa l'autorità o l'organismo di cui all'articolo 7 delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC o processi TIC certificati che possono incidere sulla conformità ai requisiti relativi alla certificazione. Tale autorità o organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersicurezza interessata.

9. Un certificato europeo di cibersicurezza è rilasciato per il periodo indicato nel sistema europeo di certificazione della cibersicurezza e può essere rinnovato, purché continuino a essere soddisfatti i requisiti pertinenti.

10. I certificati europei di cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.

Articolo 57

Sistemi e certificati nazionali di certificazione della cibersicurezza

1. Fatto salvo il paragrafo 3 del presente articolo, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC e processi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 49, paragrafo 7. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC e processi TIC non coperti da un sistema europeo di certificazione della cibersicurezza restano in vigore.

2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per prodotti TIC, servizi TIC e processi TIC già coperti da un sistema europeo di certificazione della cibersicurezza in vigore.

3. I certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza e coperti da un sistema europeo di certificazione della cibersicurezza restano validi fino alla loro data di scadenza.

4. Al fine di evitare la frammentazione del mercato interno, gli Stati membri informano la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza.

Articolo 58

Autorità nazionali di certificazione della cibersicurezza

1. Ciascuno Stato membro designa una o più autorità nazionali di certificazione della cibersicurezza nel suo territorio oppure, con l'accordo di un altro Stato membro, designa una o più autorità nazionali di certificazione della cibersicurezza stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.

2. Ciascuno Stato membro comunica alla Commissione l'identità delle autorità nazionali di certificazione della cibersicurezza designate. Se uno Stato membro designa più di una autorità, comunica alla Commissione anche i compiti assegnati a ciascuna di tali autorità.

3. Fatti salvi l'articolo 56, paragrafo 5, lettera a), e l'articolo 56, paragrafo 6, ciascuna autorità nazionale di certificazione della cibersicurezza è indipendente dai soggetti sui quali vigila per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale.

4. Gli Stati membri assicurano che le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati europei di cibersicurezza di cui all'articolo 56, paragrafo 5, lettera a), e dell'articolo 56, paragrafo 6, siano rigorosamente separate dalle attività di vigilanza indicate nel presente articolo e che tali attività siano svolte indipendentemente le une dalle altre.

5. Gli Stati membri provvedono affinché le autorità nazionali di certificazione della cibersicurezza dispongano di risorse adeguate per l'esercizio dei loro poteri e per l'esecuzione efficiente ed efficace dei loro compiti.

6. Ai fini dell'effettiva attuazione del presente regolamento, è opportuno che le autorità nazionali di certificazione della cibersicurezza partecipino in modo attivo, efficace, efficiente e sicuro all'ECCG.

7. Le autorità nazionali di certificazione della cibersicurezza:

a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti;

b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi di tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza;

c) fatto salvo l'articolo 60, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento;

d) monitorano e vigilano sulle attività degli organismi pubblici di cui all'articolo 56, paragrafo 5;

e) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità violino le prescrizioni del presente regolamento;

f) trattano i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 53, e svolgono le indagini opportune sull'oggetto di tali reclami e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole;

g) trasmettono all'ENISA e all'ECCG una relazione sintetica annuale sulle attività svolte ai sensi del presente paragrafo, lettere b), c) e d), o del paragrafo 8;

h) cooperano con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti TIC, servizi TIC e processi TIC non conformi ai requisiti del presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza; e

i) sorvegliano gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza.

8. Ciascuna autorità nazionale di certificazione della cibersicurezza dispone almeno dei seguenti poteri:

a) richiedere agli organismi di valutazione della conformità, ai titolari di certificati europei della cibersicurezza e agli emittenti di dichiarazioni UE di conformità di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;

b) condurre indagini, sotto forma di verifiche contabili, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità allo scopo di verificarne l'osservanza del presente titolo;

c) adottare misure appropriate, nel rispetto del diritto nazionale, per accertare che gli organismi di valutazione della conformità, i titolari di certificati europei di cibersicurezza e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

d) ottenere accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersicurezza al fine di svolgere indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;

e) revocare, conformemente al diritto nazionale, i certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o i certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, qualora tali certificati non siano conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

f) irrogare sanzioni conformemente al diritto nazionale, a norma dell'articolo 65, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.

9. Le autorità nazionali di certificazione della cibersicurezza cooperano tra di loro e con la Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti TIC, servizi TIC e processi TIC.

Articolo 59

Valutazione inter pares

1. Al fine di ottenere norme equivalenti in tutta l'Unione relativamente ai certificati europei di cibersicurezza e alle dichiarazioni UE di conformità, le autorità nazionali di certificazione della cibersicurezza sono soggette a una valutazione inter pares.

2. La valutazione inter pares è effettuata sulla base di criteri e procedure di valutazione solidi e trasparenti, in particolare per quanto riguarda i requisiti in termini strutturali, di risorse umane e procedurali, la riservatezza e i reclami.

3. La valutazione inter pares esamina:

a) ove applicabile, se le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati europei di cibersicurezza di cui all'articolo 56, paragrafo 5, lettera a), e all'articolo 56, paragrafo 6, siano rigorosamente separate dalle attività di vigilanza indicate all'articolo 58 e se tali attività siano svolte indipendentemente le une dalle altre;

b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i certificati europei di cibersicurezza a norma dell'articolo 58, paragrafo 7, lettera a);

c) le procedure di monitoraggio e applicazione degli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC a norma dell'articolo 58, paragrafo 7, lettera b);

d) le procedure di monitoraggio, autorizzazione e vigilanza delle attività degli organismi di valutazione della conformità;

e) ove applicabile, se il personale delle autorità o degli organismi che rilasciano certificati di livello di affidabilità «elevato» a norma dell'articolo 56, paragrafo 6, disponga di competenze adeguate.

4. La valutazione inter pares è effettuata da almeno due autorità nazionali di certificazione della cibersicurezza di altri Stati membri e dalla Commissione, e ha luogo almeno una volta ogni cinque anni. L'ENISA può partecipare alla valutazione inter pares.

5. La Commissione può adottare atti di esecuzione che definiscano un piano almeno quinquennale per la valutazione inter pares e fissino i criteri riguardanti la composizione del gruppo di valutazione inter pares, la metodologia da utilizzare in tale valutazione nonché il calendario, la frequenza e altri compiti connessi. Nell'adottare tali atti di esecuzione, la Commissione tiene debitamente conto delle opinioni dell'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

6. L'ECCG esamina i risultati delle valutazioni inter pares, redige sintesi che possono essere rese pubbliche e, se necessario, formula orientamenti o raccomandazioni in merito ad azioni o a misure che devono essere adottate dai soggetti interessati.

Articolo 60

Organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008. Tale accreditamento è rilasciato solo se l'organismo di valutazione della conformità soddisfa i requisiti indicati nell'allegato del presente regolamento.

2. Ove un certificato europeo di cibersicurezza sia rilasciato da un'autorità nazionale di certificazione della cibersicurezza a norma dell'articolo 56, paragrafo 5, lettera a), e dell'articolo 56, paragrafo 6, l'organismo di certificazione dell'autorità nazionale di certificazione della cibersicurezza è accreditato come organismo di valutazione della conformità a norma del presente articolo, paragrafo 1.

3. Qualora i sistemi europei di certificazione della cibersicurezza stabiliscano requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'autorità nazionale di certificazione della cibersicurezza a svolgere i compiti previsti da tali sistemi.

4. L'accreditamento di cui al paragrafo 1 è rilasciato agli organismi di valutazione della conformità per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni, purché l'organismo di valutazione della conformità continui a soddisfare i requisiti di cui al presente articolo. Entro un termine ragionevole, gli organismi nazionali di accreditamento adottano tutte le misure necessarie per limitare, sospendere o revocare l'accreditamento di un organismo di valutazione della conformità rilasciato in virtù del paragrafo 1 se le condizioni per l'accreditamento non sono state soddisfatte o non sono più soddisfatte oppure se l'organismo di valutazione della conformità viola il presente regolamento.

Articolo 61

Notifica

1. Per ciascun sistema europeo di certificazione della cibersicurezza le autorità nazionali di certificazione della cibersicurezza notificano alla Commissione gli organismi di valutazione della conformità che sono stati accreditati e, se del caso, autorizzati a norma dell'articolo 60, paragrafo 3, a rilasciare certificati europei di cibersicurezza a determinati livelli di affidabilità di cui all'articolo 52. Le autorità nazionali di certificazione della cibersicurezza notificano alla Commissione, senza indebito ritardo, ogni successiva modifica degli stessi.

2. Un anno dopo l'entrata in vigore di un sistema europeo di certificazione della cibersicurezza, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco degli organismi di valutazione della conformità notificati nell'ambito di tale sistema.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco degli organismi di valutazione della conformità notificati entro due mesi dalla data di ricevimento di tale notifica.

4. Un'autorità nazionale di certificazione della cibersicurezza può presentare alla Commissione una richiesta di rimozione di un organismo di valutazione della conformità notificato da tale autorità dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricevimento della richiesta dell'autorità nazionale di certificazione della cibersicurezza.

5. La Commissione può adottare atti di esecuzione per stabilire le circostanze, i formati e le procedure per le notifiche di cui al presente articolo, paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

Articolo 62

Gruppo europeo per la certificazione della cibersicurezza

1. È istituito il gruppo europeo per la certificazione della cibersicurezza («ECCG»).

2. L'ECCG è composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o da rappresentanti di altre autorità nazionali competenti. Un membro dell'ECCG non rappresenta più di due Stati membri.

3. I portatori di interessi e le parti terze interessate possono essere invitati a presenziare alle riunioni dell'ECCG e a partecipare ai suoi lavori.

4. L'ECCG ha i seguenti compiti:

a) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti del presente titolo, in particolare per quanto riguarda il programma di lavoro progressivo dell'Unione, le questioni relative alla politica in materia di certificazione della cibersicurezza, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersicurezza;

b) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema ai sensi dell'articolo 49;

c) adottare un parere sulle proposte di sistemi preparate dall'ENISA ai sensi dell'articolo 49;

d) chiedere all'ENISA di preparare proposte di sistemi ai sensi dell'articolo 48, paragrafo 2;

e) adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

f) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cibersicurezza;

g) agevolare la cooperazione tra le autorità nazionali di certificazione della cibersicurezza di cui al presente titolo attraverso lo sviluppo della capacità e lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti della certificazione della cibersicurezza;

h) sostenere l'attuazione dei meccanismi di valutazione inter pares in conformità delle regole fissate da un sistema europeo di certificazione della cibersicurezza ai sensi dell'articolo 54, paragrafo 1, lettera u);

i) agevolare l'allineamento dei sistemi europei di certificazione della cibersicurezza alle norme riconosciute a livello internazionale, rivedendo tra l'altro i sistemi europei di certificazione della cibersicurezza esistenti e, ove opportuno, rivolgendo raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale.

5. Con l'assistenza dell'ENISA, la Commissione presiede l'ECCG e svolge le funzioni di segretariato per lo stesso, conformemente all'articolo 8, paragrafo 1, lettera e).

Articolo 63

Diritto di presentare un reclamo

1. Le persone fisiche e giuridiche hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di cibersicurezza o, se il reclamo riguarda un certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità che agisce conformemente all'articolo 56, paragrafo 6, all'autorità nazionale di certificazione della cibersicurezza competente.

2. L'autorità o l'organismo a cui à stato presentato il reclamo informa il reclamante dello stato del procedimento e della decisione adottata e informa il reclamante del diritto a un ricorso giurisdizionale effettivo di cui all'articolo 64.

Articolo 64

Diritto a un ricorso giurisdizionale effettivo

1. Fatti salvi eventuali ricorsi amministrativi o altri ricorsi extragiudiziali, le persone fisiche e giuridiche hanno diritto a un ricorso giurisdizionale effettivo per quanto riguarda:

a) le decisioni assunte dall'autorità o dall'organismo di cui all'articolo 63, paragrafo 1, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cibersicurezza detenuto da tali persone fisiche e giuridiche;

b) il mancato intervento relativamente a un reclamo presentato all'autorità o all'organismo di cui all'articolo 63, paragrafo 1.

2. I procedimenti a norma del presente articolo sono presentati dinanzi ai tribunali dello Stato membro in cui ha sede l'autorità o l'organismo contro cui è mosso il ricorso giurisdizionale.

Articolo 65

Sanzioni

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

TITOLO IV

DISPOSIZIONI FINALI

Articolo 66

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5, paragrafo 4, lettera b), del regolamento (UE) n. 182/2011.

Articolo 67

Valutazione e riesame

1. Entro il 28 giugno 2024, e successivamente ogni cinque anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro fornito all'ENISA in relazione alle sue attività. Se ritiene che il mantenimento dell'ENISA non sia più giustificato alla luce degli obiettivi, del mandato e dei compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'ENISA.

2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e di migliorare il funzionamento del mercato interno.

3. La valutazione esamina se siano necessari requisiti essenziali di cibersicurezza per l'accesso al mercato interno onde impedire l'ingresso nel mercato dell'Unione di prodotti TIC, servizi TIC e processi TIC che non rispettano i requisiti di base in materia di cibersicurezza.

4. Entro il 28 giugno 2024, e successivamente ogni 5 anni, la Commissione trasmette la relazione di valutazione unitamente alle sue conclusioni al Parlamento europeo, al Consiglio e al consiglio di amministrazione. I risultati della relazione sono resi pubblici.

Articolo 68

Abrogazione e sostituzione

1. Il regolamento (UE) n. 526/2013 è abrogato con effetto a decorrere dal 27 giugno 2019.

2. I riferimenti al regolamento (UE) n. 526/2013 e all'ENISA istituita da tale regolamento si intendono fatti al presente regolamento e all'ENISA istituita dal presente regolamento.

3. L'ENISA istituita dal presente regolamento sostituisce l'ENISA istituita dal regolamento (UE) n. 526/2013 per quanto riguarda diritti di proprietà, accordi, obblighi di legge, contratti di lavoro, impegni finanziari e responsabilità. Tutte le decisioni del consiglio di amministrazione e del comitato esecutivo adottate in conformità del regolamento (UE) n. 526/2013 restano valide, purché siano conformi al presente regolamento.

4. L'ENISA è istituita per un periodo indeterminato a decorrere dal 27 giugno 2019.

5. Il direttore esecutivo nominato a norma dell'articolo 24, paragrafo 4, del regolamento (UE) n. 526/2013 resta in carica ed esercita le funzioni di direttore esecutivo ai sensi dell'articolo 20 del presente regolamento per la restante durata del mandato. Le altre condizioni contrattuali rimangono invariate.

6. I membri del consiglio di amministrazione e i loro supplenti nominati a norma dell'articolo 6 del regolamento (UE) n. 526/2013 restano in carica ed esercitano le funzioni del consiglio di amministrazione ai sensi dell'articolo 15 del presente regolamento per la restante durata del mandato.

Articolo 69

Entrata in vigore

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

2. Gli articoli 58, 60, 61, 63, 64 e 65 si applicano dal 28 giugno 2021.

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

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO

REQUISITI CHE GLI ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ DEVONO SODDISFARE

Gli organismi di valutazione della conformità che desiderano essere accreditati devono soddisfare i requisiti elencati in appresso:

1. L'organismo di valutazione della conformità è istituito a norma del diritto interno e ha personalità giuridica.

2. L'organismo di valutazione della conformità è un organismo terzo, indipendente dall'organizzazione o dai prodotti TIC, servizi TIC o processi TIC che valuta.

3. Un organismo appartenente a un'associazione d'imprese o a una federazione professionale che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura, nell'assemblaggio, nell'utilizzo o nella manutenzione dei prodotti TIC, servizi TIC o processi TIC che valuta può essere ritenuto un organismo di valutazione della conformità, a condizione che siano dimostrate la sua indipendenza e l'assenza di qualsiasi conflitto di interesse.

4. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non sono né il progettista, né il fabbricante, né il fornitore, né l'installatore, né l'acquirente, né il proprietario, né l'utilizzatore, né il responsabile della manutenzione del prodotto TIC, servizio TIC o processo TIC sottoposto a valutazione, né il rappresentante autorizzato di uno di questi soggetti. Tale divieto non preclude l'uso dei prodotti TIC valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità o il loro uso per scopi privati.

5. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intervengono direttamente nella progettazione, fabbricazione o costruzione, nella commercializzazione, nell'installazione, nell'uso o nella manutenzione dei prodotti TIC, servizi TIC o processi TIC sottoposti a valutazione, né rappresentano i soggetti impegnati in tali attività. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intraprendono attività alcuna che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle loro attività di valutazione della conformità. Tale divieto vale in particolare per i servizi di consulenza.

6. Se un organismo di valutazione della conformità è di proprietà di un ente o un'istituzione pubblici o è gestito da questi ultimi, l'indipendenza e l'assenza di conflitti di interessi tra l'autorità nazionale di certificazione della cibersicurezza e l'organismo di valutazione della conformità sono garantite e documentate.

7. Gli organismi di valutazione della conformità garantiscono che le attività delle loro affiliate e dei loro subappaltatori non abbiano effetti negativi sulla riservatezza, sull'obiettività o sull'imparzialità delle loro attività di valutazione della conformità.

8. Gli organismi di valutazione della conformità e il loro personale eseguono le attività di valutazione della conformità con il massimo dell'integrità professionale e della competenza tecnica richieste e sono liberi da qualsivoglia pressione e incentivo che possa influenzare il loro giudizio o i risultati delle loro attività di valutazione, anche pressioni e incentivi di natura finanziaria, in particolare da parte di persone o gruppi di persone interessati ai risultati di tali attività.

9. Un organismo di valutazione della conformità è in grado di effettuare tutti i compiti di valutazione della conformità ad esso attribuiti ai sensi del presente regolamento, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità. Eventuali subappalti o consultazioni di personale esterno sono adeguatamente documentati, non prevedono alcun intermediario e sono oggetto di un accordo scritto che contempli, tra l'altro, la riservatezza e i conflitti di interessi. L'organismo di valutazione della conformità in questione si assume la piena responsabilità dei compiti svolti.

10. In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo, categoria o sottocategoria di prodotti TIC, servizi TIC o processi TIC, l'organismo di valutazione della conformità dispone:

    a) di personale avente conoscenze tecniche ed esperienza sufficiente e appropriata per eseguire i compiti di valutazione della conformità;

    b) di descrizioni delle procedure in base alle quali si svolge la valutazione della conformità, si garantisce la trasparenza di tali procedure e la possibilità di riprodurle. Predispone una politica e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato ai sensi dell'articolo 61 dalle altre attività;

c) di procedure per svolgere le attività che tengano debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto TIC, servizio TIC o processo TIC in questione e della natura di massa o seriale del processo produttivo.

11. L'organismo di valutazione della conformità dispone dei mezzi necessari per eseguire i compiti tecnici e amministrativi connessi alle attività di valutazione della conformità in modo appropriato e ha accesso a tutti gli strumenti e impianti occorrenti.

12. Le persone addette alle attività di valutazione della conformità dispongono di quanto segue:

a) una formazione tecnica e professionale solida che includa tutte le attività di valutazione della conformità;

b) soddisfacenti conoscenze delle prescrizioni relative alle valutazioni della conformità che eseguono e un'adeguata autorità per eseguire tali valutazioni;

c) una conoscenza e una comprensione adeguate dei requisiti e delle norme di prova applicabili;

d) la capacità di elaborare certificati, registri e relazioni a dimostrazione del fatto che le valutazioni sono state effettuate.

13. È garantita l'imparzialità dell'organismo di valutazione della conformità, dei suoi alti dirigenti, delle persone addette alle attività di valutazione della conformità e di tutti i subcontraenti.

14. La remunerazione degli alti dirigenti e delle persone addette alle attività di valutazione della conformità non dipende dal numero di valutazioni della conformità eseguite o dai risultati di tali valutazioni.

15. Gli organismi di valutazione della conformità sottoscrivono un contratto di assicurazione per la responsabilità civile, a meno che detta responsabilità non sia direttamente coperta dallo Stato membro a norma del diritto nazionale o che lo Stato membro stesso non sia direttamente responsabile della valutazione della conformità.

16. L'organismo di valutazione della conformità e il personale, i comitati, le controllate e i subcontraenti dello stesso e qualsiasi organismo associato o membro del personale di organismi esterni di un organismo di valutazione della conformità sono tenuti al mantenimento della riservatezza e al segreto professionale per tutto ciò di cui vengono a conoscenza nell'esercizio dei loro compiti di valutazione della conformità ai sensi del presente regolamento o di qualsiasi disposizione di diritto interno di applicazione del presente regolamento, tranne laddove la divulgazione sia richiesta dal diritto dell'Unione o dello Stato membro cui tali persone sono soggette, e tranne per quanto riguarda le autorità competenti degli Stati membri in cui esercitano le loro attività. Sono tutelati i diritti di proprietà intellettuale. L'organismo di valutazione della conformità dispone di procedure documentate riguardo ai requisiti di cui al presente punto.

17. Con l'eccezione del punto 16, i requisiti del presente allegato non precludono in alcun modo gli scambi di informazioni tecniche e di orientamenti regolamentari tra un organismo di valutazione della conformità e una persona che richieda la certificazione o stia valutando se richiedere la certificazione.

18. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque e ragionevoli, tenendo conto degli interessi delle PMI in relazione alle tariffe.

19. Gli organismi di valutazione della conformità sono conformi ai requisiti della pertinente norma armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità che effettuano la certificazione dei prodotti TIC, servizi TIC o processi TIC.

20. Gli organismi di valutazione della conformità si assicurano che i laboratori di prova utilizzati ai fini della valutazione della conformità siano conformi ai requisiti della pertinente norma armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento dei laboratori che effettuano prove.