

Il presente testo è un semplice strumento di documentazione e non produce alcun effetto giuridico. Le istituzioni dell'Unione non assumono alcuna responsabilità per i suoi contenuti. Le versioni facenti fede degli atti pertinenti, compresi i loro preamboli, sono quelle pubblicate nella Gazzetta ufficiale dell'Unione europea e disponibili in EUR-Lex. Tali testi ufficiali sono direttamente accessibili attraverso i link inseriti nel presente documento

► **B** **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)

(GU L 151 del 7.6.2019, pag. 15)

Modificato da:

Gazzetta ufficiale

		n.	pag.	data
► <u>M1</u>	Regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio del 19 dicembre 2024	L 37	1	15.1.2025

▼B**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)****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

▼M1

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

▼B

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;

▼B

- 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;

▼M1

- 9) «sistema europeo di certificazione della cibersecurity»: una serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti;
- 10) «sistema nazionale di certificazione della cibersecurity»: una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti che rientrano nell'ambito di applicazione del sistema specifico;
- 11) «certificato europeo di cibersecurity»: un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito è stato oggetto di una valutazione di conformità ai requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersecurity;

▼B

- 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;

▼M1

- 14 bis) «servizio di sicurezza gestito»: un servizio prestato a un terzo consistente nello svolgimento di attività, o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cibersecurity, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica;

▼B

- 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;

▼M1

- 20) «specificata tecnica»: un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC, un processo TIC o un servizio di sicurezza gestito 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, processo TIC o servizio di sicurezza gestito soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersecurity e indica il livello al quale un prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito interessato;
- 22) «autovalutazione di conformità»: un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti che valuta se tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersecurity.

▼B

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 cibersecurity in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersecurity. L'ENISA funge da punto di riferimento per pareri e competenze in materia di cibersecurity per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione.

▼B

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 cibersecurity.

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 attribuiti ai sensi del presente regolamento.

*Articolo 4***Obiettivi**

1. L'ENISA opera come centro di competenze nel campo della cibersecurity 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 cibersecurity, ivi comprese le politiche settoriali in materia di cibersecurity.

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 cyberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersecurity.

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 cibersecurity.

5. L'ENISA contribuisce a rafforzare le capacità di cibersecurity 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.

▼M1

6. L'ENISA promuove l'uso della certificazione europea della cibersecurity, 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 cibersecurity, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti in termini di cibersecurity, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.

▼B

7. L'ENISA promuove un elevato livello di consapevolezza in materia di cibersecurity, 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 cibersecurity e delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cibersecurity, 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 cibersecurity, 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 cibersecurity 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 cibersecurity 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;

▼B

- 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 ⁽¹⁾;
 - 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.

*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;

⁽¹⁾ 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).

▼B

- 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 inter-settoriale, 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.

▼B

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

- 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****▼M1**

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, dei processi TIC e dei servizi di sicurezza gestiti, come stabilito al titolo III del presente regolamento:

▼B

- 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;

▼M1

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

▼B

- 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.

▼M1

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

▼B

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.

▼M1

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, dei processi TIC e dei servizi di sicurezza gestiti.

▼B

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

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

*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 cibersecurity, 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 cibersecurity.

*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 cibersecurity:

- 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;

▼B

- 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 1° luglio dell'anno successivo, sia la relazione annuale che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti, 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;

▼B

- 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, CEEA) n. 259/68 del Consiglio ⁽¹⁾ 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.

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.

⁽¹⁾ GU L 56 del 4.3.1968, pag. 1.

*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.

▼B

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.

▼B

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;

▼B

- 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.

▼B

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.

▼B

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.

▼B

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

F u n z i o n a m e n t o

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 ⁽¹⁾.

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.

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.

⁽¹⁾ 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).

▼B

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.

▼B*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 ⁽¹⁾ e 2015/444 ⁽²⁾ 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.

⁽¹⁾ Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

⁽²⁾ 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).

▼B

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.

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 1° 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 ⁽¹⁾, 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 1° 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.
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 scarico per l'esercizio in causa, in conformità dell'articolo 261, paragrafo 3, del regolamento (UE, Euratom) 2018/1046.

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

▼B

12. Il Parlamento europeo, su raccomandazione del Consiglio, concede il discharge 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 ⁽¹⁾, 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) ⁽²⁾. 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 ⁽³⁾, 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.

⁽¹⁾ 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).

⁽²⁾ GU L 136 del 31.5.1999, pag. 15.

⁽³⁾ 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.

▼B

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.

▼B

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 ⁽¹⁾. 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.

*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.

⁽¹⁾ Regolamento del Consiglio n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU L7 del 6.10.1958, pag. 385).

▼B

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**

Prevvia consultazione della Commissione, l'ENISA adotta regole in materia di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni sensibili non classificate e delle ICUE di cui alle decisioni (UE, Euratom) 2015/443 e 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.

▼B

TITOLO III

QUADRO DI CERTIFICAZIONE DELLA CIBERSICUREZZA**▼M1***Articolo 46***Quadro europeo di certificazione della cibersecurity**

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

2. Il quadro europeo di certificazione della cibersecurity prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersecurity e ad attestare che i prodotti TIC, i servizi TIC e i processi TIC valutati nell'ambito di tali sistemi siano 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. Esso attesta, inoltre, che i servizi di sicurezza gestiti valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza ai fini della protezione della disponibilità, dell'autenticità, dell'integrità e della riservatezza dei dati consultati, trattati, conservati o trasmessi in relazione alla prestazione di tali servizi, e che tali servizi sono forniti continuamente con la competenza, la perizia e l'esperienza richieste da personale avente un livello sufficiente e adeguato di conoscenze tecniche pertinenti e integrità professionale.

▼B*Articolo 47***Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersecurity**

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

▼M1

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

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

▼ M1

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

▼ B

- b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri;
- c) la domanda di mercato;

▼ M1

- c *bis*) gli sviluppi tecnologici nonché la disponibilità e lo sviluppo di sistemi internazionali di certificazione della cibersecurity e di norme internazionali e norme utilizzate dall'industria;

▼ B

- d) gli sviluppi nel panorama delle minacce informatiche;
- e) la richiesta di preparazione di una specifica proposta di sistema da parte dell'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 cibersecurity.

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 cibersecurity**

1. La Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersecurity 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 cibersecurity 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 cibersecurity****▼ M1**

1. A seguito di una richiesta della Commissione a norma dell'articolo 48, l'ENISA prepara una proposta di sistema che soddisfi i requisiti applicabili di cui agli articoli 51, 51 bis, 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 applicabili di cui agli articoli 51, 51 bis, 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.

▼ M1

3. In sede di preparazione di una proposta di sistema, l'ENISA consulta tempestivamente tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo. Quando trasmette la proposta di sistema alla Commissione a norma del paragrafo 6, l'ENISA fornisce informazioni sulle modalità con cui ha sì è conformata a tale paragrafo.

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. Tali gruppi di lavoro ad hoc comprendono, se del caso e fatte salve le procedure e la discrezionalità previste dall'articolo 20, paragrafo 4, esperti delle amministrazioni pubbliche degli Stati membri, delle istituzioni, degli organi e degli organismi dell'Unione, nonché del settore privato.

▼ B

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.

▼ M1

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, i processi TIC e i servizi di sicurezza gestiti che soddisfa i requisiti pertinenti di cui agli articoli 51, 51 bis, 52 e 54. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

▼ B

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.

▼ M1*Articolo 49 bis***Informazione e consultazione sui sistemi europei di certificazione della cibersicurezza**

1. La Commissione rende pubbliche le informazioni concernenti la sua richiesta all'ENISA relativa alla preparazione di una proposta di sistema o alla revisione di un sistema europeo di certificazione della cibersicurezza esistente di cui all'articolo 48.

▼ M1

2. Nel corso della preparazione di una proposta di sistema da parte dell'ENISA a norma dell'articolo 49, il Parlamento europeo, il Consiglio o entrambi possono chiedere alla Commissione, in qualità di presidente dell'ECCG, e all'ENISA di presentare, su base trimestrale, le pertinenti informazioni relative a un progetto di proposta di sistema. Su richiesta del Parlamento europeo o del Consiglio, l'ENISA, d'intesa con la Commissione e fatto salvo l'articolo 27, può mettere a disposizione del Parlamento europeo e del Consiglio le parti pertinenti di un progetto di proposta di sistema con modalità adeguate al livello di riservatezza richiesto e, se del caso, limitate.

3. Al fine di rafforzare il dialogo tra le istituzioni dell'Unione e di contribuire a un processo di consultazione formale, aperto, trasparente e inclusivo, il Parlamento europeo, il Consiglio o entrambi possono invitare la Commissione e l'ENISA a discutere questioni relative al funzionamento dei sistemi europei di certificazione della cibersecurity per prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti.

4. Nel valutare il presente regolamento a norma dell'articolo 67, la Commissione tiene conto, se del caso, degli elementi derivanti dai pareri espressi dal Parlamento europeo e dal Consiglio sulle questioni di cui al paragrafo 3 del presente articolo.

▼ B*Articolo 50***Sito web sui sistemi europei di certificazione della cibersecurity**

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

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

*Articolo 51***▼ M1****Obiettivi di sicurezza dei sistemi europei di certificazione della cibersecurity per i prodotti TIC, i servizi TIC e i processi TIC**

I sistemi europei di certificazione della cibersecurity per i prodotti TIC, i servizi TIC o i processi TIC sono progettati per conseguire, a seconda del caso, almeno gli obiettivi di sicurezza seguenti:

▼B

- 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.

▼M1*Articolo 51 bis***Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti**

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

- a) che i servizi di sicurezza gestiti siano forniti con la competenza, la perizia e l'esperienza richieste e il personale responsabile della prestazione di tali servizi possieda un livello sufficiente e adeguato di conoscenze e competenze tecniche nel settore specifico, un'esperienza sufficiente e appropriata e la massima integrità professionale;

▼ M1

- b) che il fornitore predisponga procedure interne appropriate affinché i servizi di sicurezza gestiti forniti abbiano sempre un livello di qualità sufficiente e adeguato;
- c) che i dati consultati, conservati, trasmessi o altrimenti trattati in relazione alla fornitura dei servizi di sicurezza gestiti siano protetti contro l'accesso, l'archiviazione, la divulgazione, la distruzione o altro tipo di trattamento, accidentali o non autorizzati, la perdita o l'alterazione o la mancanza di disponibilità;
- d) che la disponibilità dei dati, dei servizi e delle funzioni e l'accesso agli stessi siano ripristinati in modo tempestivo in caso di incidente fisico o tecnico;
- e) che le persone, i programmi o le macchine autorizzati possano accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;
- f) che sia conservata una registrazione, disponibile per la valutazione, dei dati, dei servizi o delle funzioni per i quali è stato effettuato l'accesso, e che sono stati utilizzati o altrimenti trattati, in quale momento e da chi;
- g) che i prodotti TIC, i servizi TIC e i processi TIC avviati nella fornitura dei servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita e, se del caso, includano gli ultimi aggiornamenti connessi alla sicurezza e non contengano vulnerabilità note.

▼ B*Articolo 52***Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza****▼ M1**

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

▼ B

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.

▼ M1

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, processo TIC o servizio di sicurezza gestito.

▼B

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

▼M1

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, i processi TIC o i servizi di sicurezza gestiti 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, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per i quali è rilasciato 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, i processi TIC o i servizi di sicurezza gestiti 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, i processi TIC o i servizi di sicurezza gestiti per i quali è rilasciato 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, i processi TIC o i servizi di sicurezza gestiti 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.

▼B

8. I sistemi europei di certificazione della cibersecurity 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'ideale combinazione di componenti dell'affidabilità.

*Articolo 53***Autovalutazione della conformità****▼M1**

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

2. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti 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, processi TIC o servizi di sicurezza gestiti si assume la responsabilità della conformità del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito ai requisiti previsti in tale sistema.

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

▼B

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 cibersecurity**

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

▼M1

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

▼B

- 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 cibersecurity definiti nel sistema europeo di certificazione della cibersecurity;
- 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 cibersecurity;

▼M1

- 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 agli articoli 51 e 51 bis sono stati conseguiti;

▼B

- 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;

▼M1

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

▼B

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

▼M1

- l) le regole riguardanti le conseguenze per i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti 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;

▼B

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

▼B

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

▼M1

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

▼B

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

▼M1

- q) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti che devono essere rese disponibili dal fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti;

▼B

- r) il periodo massimo di validità dei certificati europei di cibersecurity rilasciati nell'ambito del sistema;
- s) la politica di divulgazione dei certificati europei di cibersecurity 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 cibersecurity 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 cibersecurity a norma dell'articolo 55.

2. I requisiti specificati del sistema europeo di certificazione della cibersecurity 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 cibersecurity 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 cibersecurity possa essere utilizzato per stabilire la presunzione di conformità agli obblighi di legge.

▼B*Articolo 55***Informazioni supplementari sulla cibersecurity dei prodotti TIC, servizi TIC e processi TIC certificati**

1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC 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 cibersecurity:

- 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 cibersecurity;
- 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 cibersecurity.

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 cibersecurity o della dichiarazione UE di conformità corrispondenti.

*Articolo 56***Certificazione della cibersecurity****▼M1**

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

▼B

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

3. ►**M1** La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersecurity adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersecurity mediante pertinenti disposizioni di diritto dell'Unione al fine di garantire l'opportuno livello di cibersecurity nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC e, a decorrere dal 4 febbraio 2025, dei servizi di sicurezza gestiti 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, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione. ◀

▼B

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 cibersecurity.

Nel preparare la valutazione la Commissione:

▼M1

a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti 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, i processi TIC o i servizi di sicurezza gestiti in questione;

▼B

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;

▼M1

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 fabbricanti o fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, compresi gli interessi e i fabbisogni specifici delle PMI, incluse le microimprese;

▼B

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 cibersecurity 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 cibersecurity adottato dalla Commissione a norma dell'articolo 49.

5. In deroga al paragrafo 4, in casi debitamente giustificati un sistema europeo di certificazione della cibersecurity può prevedere che i certificati europei di cibersecurity 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 cibersecurity 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.

▼B

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

- a) previa approvazione dell'autorità nazionale di certificazione della cibersecurity per ogni singolo certificato europeo di cibersecurity rilasciato da un organismo di valutazione della conformità; o
- b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cibersecurity a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersecurity.

▼M1

7. La persona fisica o giuridica che presenta i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per la certificazione mette a disposizione dell'autorità nazionale di certificazione della cibersecurity designata a norma dell'articolo 58, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersecurity, 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 cibersecurity informa l'autorità o l'organismo di cui al paragrafo 7 delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti 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 cibersecurity interessata.

▼B

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

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

*Articolo 57***Sistemi e certificati nazionali di certificazione della cibersecurity****▼M1**

1. Fatto salvo il paragrafo 3 del presente articolo, i sistemi nazionali di certificazione della cibersecurity e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti coperti da un sistema europeo di certificazione della cibersecurity 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 cibersecurity e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti non coperti da un sistema europeo di certificazione della cibersecurity restano in vigore.

▼M1

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

▼B

3. I certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersecurity e coperti da un sistema europeo di certificazione della cibersecurity 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 cibersecurity.

*Articolo 58***Autorità nazionali di certificazione della cibersecurity**

1. Ciascuno Stato membro designa una o più autorità nazionali di certificazione della cibersecurity nel suo territorio oppure, con l'accordo di un altro Stato membro, designa una o più autorità nazionali di certificazione della cibersecurity 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 cibersecurity 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 cibersecurity è indipendente dai soggetti sui quali vigila per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale.

4. Gli Stati membri assicurano che le attività delle autorità nazionali di certificazione della cibersecurity relative al rilascio di certificati europei di cibersecurity 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 cibersecurity 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 cibersecurity partecipino in modo attivo, efficace, efficiente e sicuro all'ECCG.

▼B

7. Le autorità nazionali di certificazione della cibersecurity:

▼M1

a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersecurity a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti ai requisiti dei certificati europei di cibersecurity 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, processi TIC o servizi di sicurezza gestiti che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, e in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi incombenti a tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersecurity;

▼B

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 cibersecurity rilasciati dalle autorità nazionali di certificazione della cibersecurity o ai certificati europei di cibersecurity 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;

▼M1

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

▼B

- 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.

▼M1

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, processi TIC e servizi di sicurezza gestiti.

▼B*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.

▼B

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;

▼M1

b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti 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, processi TIC o servizi di sicurezza gestiti a norma dell'articolo 58, paragrafo 7, lettera b);

▼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 cibersecurity sia rilasciato da un'autorità nazionale di certificazione della cibersecurity 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 cibersecurity è accreditato come organismo di valutazione della conformità a norma del presente articolo, paragrafo 1.
3. Qualora i sistemi europei di certificazione della cibersecurity 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 cibersecurity 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 cibersecurity le autorità nazionali di certificazione della cibersecurity 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 cibersecurity a determinati livelli di affidabilità di cui all'articolo 52. Le autorità nazionali di certificazione della cibersecurity 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 cibersecurity, 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.

▼B

4. Un'autorità nazionale di certificazione della cibersecurity 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 cibersecurity.

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 cibersecurity**

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

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

3. 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 cibersecurity, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersecurity;
- 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 cibersecurity.
- f) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersecurity e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cibersecurity;

▼B

- 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 è 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.

▼B*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.

▼M1

2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento, incluse le procedure che portano all'adozione dei sistemi europei di certificazione della cibersicurezza e le loro basi probatorie, per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti 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 interno di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che non rispettano i requisiti di base in materia di cibersicurezza.

▼B

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.

▼B*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.

▼M1

2. L'organismo di valutazione della conformità è un organismo terzo, indipendente dall'organizzazione o dai prodotti TIC, dai servizi TIC, dai processi TIC o dai servizi di sicurezza gestiti che valuta.
3. Un organismo appartenente a un'associazione d'impresa 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, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti 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, del servizio TIC, del processo TIC o del servizio di sicurezza gestito 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 fornitura, nella commercializzazione, nell'installazione, nell'uso o nella manutenzione dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti 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.

▼B

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.

▼ B

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.

▼ M1

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

▼ B

- 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. Predisporre una politica e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato ai sensi dell'articolo 61 dalle altre attività;

▼ M1

- 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, processo TIC o servizio di sicurezza gestito in questione e della natura di massa o seriale del processo produttivo.

▼ B

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.

▼B

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.

▼M1

19. Gli organismi di valutazione della conformità sono conformi ai requisiti della pertinente norma armonizzata quale definita all'articolo 2, punto 9), del regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità che effettuano la certificazione dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti.
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 quale definita all'articolo 2, punto 9), del regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento dei laboratori che effettuano prove.