DECISIONE (UE) 2022/640 DELLA COMMISSIONE

del 7 aprile 2022

sulle norme di attuazione concernenti i ruoli e le responsabilità dei principali operatori della sicurezza

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 249,

vista la decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione ([1]),

vista la decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE ([2]),

considerando quanto segue:

(1) Le decisioni (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444 si applicano a tutti i servizi e in tutti i locali della Commissione.

(2) Laddove necessario devono essere adottate norme di attuazione intese a integrare o sostenere la decisione (UE, Euratom) 2015/444 in conformità dell'articolo 60 della medesima.

(3) Le misure di sicurezza per proteggere le informazioni classificate UE nel corso del loro ciclo di vita dovrebbero essere commisurate in particolare alla rispettiva classifica di sicurezza.

(4) Le misure di sicurezza per proteggere i sistemi di comunicazione e informazione della Commissione sono stabilite nella decisione (UE, Euratom) 2017/46 della Commissione ([3]), in particolare all'articolo 3 relativo ai principi per la sicurezza informatica alla Commissione e all'articolo 9 relativo ai proprietari dei sistemi.

(5) L'obiettivo delle norme di attuazione concernenti i ruoli e le responsabilità dei principali operatori della sicurezza è orientare sui presupposti e sulle mansioni stabiliti per tali ruoli nelle decisioni (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444.

(6) L'articolo 36, paragrafo 7, della decisione (UE, Euratom) 2015/444 elenca una serie di funzioni aggiuntive legate alla sicurezza che devono essere assegnate all'autorità di sicurezza della Commissione. I compiti associati a tali funzioni sono definiti nella presente decisione.

(7) In conformità della decisione (UE, Euratom) 2015/444 i responsabili locali della sicurezza e i funzionari responsabili del controllo delle registrazioni hanno responsabilità specifiche in materia di protezione delle informazioni classificate UE nei rispettivi servizi.

(8) Il 4 maggio 2016 la Commissione ha adottato una decisione ([4]) che abilita il membro della Commissione responsabile per le questioni di sicurezza ad adottare, a nome della Commissione e sotto la sua responsabilità, le norme di attuazione di cui all'articolo 60 della decisione (UE, Euratom) 2015/444; il 13 aprile 2021 il membro della Commissione responsabile per le questioni di sicurezza ha poi adottato, a nome della Commissione e sotto la sua responsabilità, una decisione ([5]) che subdelega al direttore generale delle Risorse umane e della sicurezza i poteri per l'adozione di tali norme di attuazione,

([1]) GU L 72 del 17.3.2015, pag. 41.
([2]) GU L 72 del 17.3.2015, pag. 53.
([3]) Decisione (UE, Euratom) 2017/46 della Commissione, del 10 gennaio 2017, sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea (GU L 6 dell'11.1.2017, pag. 40).
([4]) Decisione C(2016) 2797 della Commissione, del 4 maggio 2016, relativa alla delega di poteri in materia di sicurezza.
([5]) Decisione C(2021) 2684 della Commissione, del 13 aprile 2021, che subdelega i poteri conferiti con la decisione C(2016)2797 della Commissione relativa alla delega di poteri in materia di sicurezza.

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

Disposizioni generali

Articolo 1

Oggetto e ambito di applicazione

1. La presente decisione stabilisce i ruoli e le responsabilità dei principali operatori della sicurezza cui compete la protezione delle informazioni classificate UE (ICUE) nella Commissione a norma delle decisioni (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444.

2. La presente decisione si applica a tutti i servizi e in tutti i locali della Commissione.

CAPO 2

Direzione generale Risorse umane e sicurezza

Articolo 2

Autorità di sicurezza della Commissione

1. Il direttore della direzione Sicurezza della direzione generale Risorse umane e sicurezza è l'autorità di sicurezza della Commissione di cui all'articolo 7 della decisione (UE, Euratom) 2015/444.

2. L'autorità di sicurezza della Commissione espleta le sue funzioni nei seguenti ambiti definiti nella decisione (UE, Euratom) 2015/444, in conformità degli articoli da 3 a 7 della presente decisione:

a) sicurezza del personale;

b) sicurezza materiale;

c) gestione delle ICUE;

d) accreditamento di qualsiasi sistema di comunicazione e informazione (CIS) che tratta ICUE;

e) sicurezza industriale; e

f) scambio di informazioni classificate.

3. L'autorità di sicurezza della Commissione impartisce ai responsabili locali della sicurezza (LSO), agli LSO aggiunti, ai funzionari responsabili del controllo delle registrazioni (RCO) e agli RCO aggiunti la formazione obbligatoria sulle rispettive responsabilità e mansioni.

Articolo 3

Autorità per la garanzia di sicurezza delle informazioni

L'autorità per la garanzia di sicurezza delle informazioni è responsabile delle seguenti attività con riferimento alla protezione delle ICUE:

a) elaborare politiche e orientamenti di sicurezza in materia di garanzia di sicurezza delle informazioni e monitorarne l'efficacia e la pertinenza;

b) salvaguardare e gestire informazioni tecniche relative ai prodotti crittografici;

c) provvedere affinché le misure in materia di garanzia di sicurezza delle informazioni siano conformi alle politiche della Commissione in materia di sicurezza e di appalti;

d) garantire che i prodotti crittografici siano selezionati nel rispetto delle politiche che ne disciplinano l'ammissibilità e la selezione;

e) consultare i proprietari di sistemi, i fornitori di sistemi, gli operatori della sicurezza e i rappresentanti degli utenti per quanto riguarda le politiche e gli orientamenti di sicurezza in materia di garanzia di sicurezza delle informazioni.

Articolo 4

Autorità di accreditamento di sicurezza

1. L'autorità di sicurezza della Commissione è responsabile dell'accreditamento delle zone protette conformi ai requisiti di cui all'articolo 18 della decisione (UE, Euratom) 2015/444 e dell'accreditamento dei CIS per il trattamento delle ICUE.

2. Ciascun servizio della Commissione consulta, in coordinamento con il proprio LSO o con il proprio responsabile della sicurezza informatica a livello locale (LISO) secondo il caso, l'autorità di accreditamento di sicurezza ogniqualvolta intende:

a) allestire una zona protetta;

b) approntare un CIS per il trattamento di ICUE;

c) installare qualsiasi altra attrezzatura per il trattamento di informazioni classificate, compreso il collegamento con un CIS di terzi.

L'autorità di accreditamento di sicurezza offre consulenza sulle attività elencate, nelle fasi di pianificazione e di allestimento così come di sviluppo.

3. Le ICUE sono trattate in una zona protetta o in un CIS soltanto previo accreditamento rilasciato dall'autorità di accreditamento di sicurezza per il livello di ICUE adeguato.

4. Sono presupposti indispensabili dell'accreditamento della zona protetta:

a) l'approvazione dei piani per la zona protetta;

b) l'approvazione di qualsiasi contratto d'opera per lavori eseguiti da contraenti esterni, tenuto conto delle disposizioni in materia di sicurezza industriale quali l'obbligo di nulla osta di sicurezza dei contraenti e del relativo personale;

c) la disponibilità di tutte le dichiarazioni e di tutti i certificati di conformità necessari;

d) un'ispezione fisica della zona protetta per verificare che i materiali e i metodi di costruzione, i controlli dell'accesso, le attrezzature di sicurezza e ogni altro elemento soddisfino i requisiti stabiliti dall'autorità di sicurezza della Commissione;

e) la convalida delle misure contro le radiazioni elettromagnetiche per qualsiasi zona protetta tecnicamente;

f) l'approvazione delle procedure operative di sicurezza (SecOP) per la zona protetta.

5. Sono presupposti indispensabili dell'accreditamento del CIS che tratta ICUE:

a) la definizione di una strategia di accreditamento del sistema;

b) la convalida del piano di sicurezza del CIS in linea con un approccio di gestione del rischio;

c) la convalida delle SecOP per il CIS;

d) la convalida di ogni altra documentazione di sicurezza necessaria, stabilita dall'autorità di accreditamento di sicurezza;

e) l'approvazione dell'impiego di tecnologie di crittografia;

f) la convalida delle misure contro le radiazioni elettromagnetiche per il CIS che tratta informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore;

g) l'ispezione del CIS per verificare la corretta attuazione delle misure di sicurezza documentate.

6. Se i requisiti per l'accreditamento sono soddisfatti, l'autorità di accreditamento di sicurezza rilascia l'autorizzazione ufficiale per il trattamento delle ICUE nella zona protetta o nel CIS, per un dato livello massimo di ICUE e per un periodo non superiore a cinque anni, a seconda del livello delle ICUE trattate e dei rischi collegati.

7. Se è notificata una violazione della sicurezza o una variazione consistente della progettazione o delle misure di sicurezza della zona protetta o del CIS, l'autorità di accreditamento di sicurezza riesamina l'autorizzazione di trattare ICUE e, se del caso, può revocarla fino alla risoluzione dei problemi riscontrati.

Articolo 5

Autorità TEMPEST

1. Sono attuate misure di sicurezza TEMPEST per proteggere i CIS che trattano informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore; misure TEMPEST possono essere attuate per le informazioni classificate di livello RESTREINT UE/EU RESTRICTED.

2. L'autorità TEMPEST è responsabile dell'approvazione delle misure di protezione adottate per evitare che le ICUE siano compromesse da emissioni elettroniche non intenzionali.

3. Su richiesta del proprietario di un sistema CIS che tratta ICUE, l'autorità TEMPEST emana opportune specifiche per le misure di sicurezza TEMPEST in base al livello di classifica delle informazioni.

4. L'autorità TEMPEST esegue prove tecniche durante il processo di accreditamento delle zone protette e dei CIS per il trattamento di ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore e, una volta concluse con esito positivo le prove, rilascia un certificato TEMPEST.

5. Il certificato TEMPEST riporta almeno le informazioni seguenti:

a) data di esecuzione della prova;

b) descrizione delle misure di sicurezza TEMPEST, corredate di pianta dei locali;

c) data di scadenza del certificato;

d) eventuali variazioni che invalideranno la certificazione;

e) firma dell'autorità TEMPEST.

6. L'LSO o l'organizzatore di riunioni incaricato di organizzare una riunione classificata, in coordinamento con l'LSO, può chiedere all'autorità TEMPEST di sottoporre a prova la sala riunioni per accertare che sia protetta tecnicamente.

Articolo 6

Autorità di approvazione degli apparati crittografici

1. L'autorità di approvazione degli apparati crittografici è incaricata di approvare l'uso di tecnologie di crittografia.

2. L'autorità di approvazione degli apparati crittografici emana orientamenti relativi ai requisiti per l'impiego e l'approvazione di tecnologie di crittografia.

3. L'autorità di approvazione degli apparati crittografici approva l'impiego di soluzioni di crittografia sulla scorta di una richiesta del proprietario del sistema. L'approvazione presuppone una valutazione soddisfacente almeno per quanto riguarda gli aspetti seguenti:

a) le esigenze di sicurezza delle informazioni da proteggere;

b) una panoramica del CIS interessato dalla soluzione;

c) una valutazione del rischio intrinseco e del rischio residuo;

d) la descrizione della soluzione proposta;

e) le SecOP per la soluzione di crittografia.

4. L'autorità di approvazione degli apparati crittografici conserva un registro delle soluzioni di crittografia approvate.

Articolo 7

Autorità di distribuzione degli apparati crittografici

1. L'autorità di distribuzione degli apparati crittografici è responsabile della distribuzione del materiale crittografico utilizzato per la protezione delle ICUE (principalmente dispositivi di cifratura, chiavi crittografiche, certificati e relativi autenticatori) ai soggetti seguenti:

a) utenti o servizi interni alla Commissione per i CIS gestiti da soggetti esterni;

b) utenti o organizzazioni esterni alla Commissione per i CIS gestiti dalla Commissione.

2. L'autorità di distribuzione degli apparati crittografici può, a norma dell'articolo 17, paragrafo 3, della decisione 2015/443, delegare ad altri servizi la distribuzione del materiale crittografico per soggetti terzi.

3. L'autorità di distribuzione degli apparati crittografici provvede affinché tutto il materiale crittografico sia inviato mediante canali sicuri in grado di prevenire e rilevare manomissioni, in conformità delle norme di sicurezza applicabili per il livello di classifica delle ICUE destinate ad essere protette per mezzo di tale materiale.

4. L'autorità di distribuzione degli apparati crittografici offre orientamento all'LSO e, se del caso, al responsabile della sicurezza informatica a livello locale di ciascun servizio della Commissione che partecipa alla produzione, alla distribuzione o all'impiego del materiale crittografico.

5. L'autorità di distribuzione degli apparati crittografici provvede affinché siano stabilite SecOP idonee per il processo di distribuzione.

CAPO 3

Servizi della Commissione

Articolo 8

Caposervizio

1. Ciascun caposervizio nomina:

a) un LSO e uno o più LSO aggiunti ove opportuno per il servizio o gabinetto;

b) un RCO e uno o più RCO aggiunti ove opportuno per il servizio che gestisce un ufficio di registrazione delle ICUE;

c) un proprietario del sistema per ciascun CIS che tratta ICUE.

2. Prima di procedere alla nomina degli LSO, degli LSO aggiunti, degli RCO e degli RCO aggiunti il caposervizio chiede l'approvazione del direttore della direzione Sicurezza della direzione generale Risorse umane e sicurezza.

3. Il caposervizio individua, in consultazione con l'LSO, tutti i posti per i quali è necessario un nulla osta per l'accesso alle ICUE. I candidati a tali posti sono informati dell'obbligo di nulla osta nel corso dell'iter di assunzione.

4. Il capo del servizio che detiene ICUE è responsabile di attivare, ove necessario, i piani di distruzione e di evacuazione di emergenza. I piani prevedono un'alternativa per le situazioni in cui non sia possibile contattare il caposervizio.

Articolo 9

Proprietari di CIS che trattano ICUE

1. Il proprietario del sistema contatta l'autorità di accreditamento di sicurezza in una fase il più possibile precoce del progetto per l'attuazione di un CIS che tratta ICUE, al fine di stabilire le necessarie norme e i requisiti di sicurezza e di avviare la procedura di accreditamento di sicurezza.

2. Il proprietario del sistema provvede a che le misure di sicurezza soddisfino i requisiti definiti dall'autorità di accreditamento di sicurezza e che il CIS non tratti ICUE prima di essere stato accreditato.

3. Il proprietario del sistema contatta l'autorità di approvazione degli apparati crittografici per richiedere l'autorizzazione di impiegare tecnologie di crittografia. Il proprietario del sistema mette in funzione tecnologie di crittografia nei sistemi di produzione soltanto previa approvazione.

4. Il proprietario del sistema consulta il LISO del servizio sulle questioni inerenti alla sicurezza del CIS.

5. Il proprietario del sistema riesamina le misure di sicurezza applicate al sistema, compreso il relativo piano di sicurezza, almeno con frequenza annuale.

6. Qualora in un CIS si verifichi un incidente di sicurezza a seguito del quale risulti evidente che il CIS non è più in grado di proteggere adeguatamente le ICUE, il proprietario del sistema informa l'LSO e contatta immediatamente l'autorità di accreditamento di sicurezza chiedendo consiglio sulle misure da adottare. Nella citata eventualità l'accreditamento può essere sospeso e il sistema può essere messo fuori servizio fino ad adozione di idoneo intervento correttivo.

7. Il proprietario del sistema offre in ogni momento totale sostegno all'autorità di accreditamento di sicurezza nell'espletamento delle funzioni che le incombono per l'accreditamento del CIS.

Articolo 10

Autorità operativa per la garanzia di sicurezza delle informazioni

Per ciascun CIS l'autorità operativa per la garanzia di sicurezza delle informazioni provvede a:

a) elaborare una documentazione di sicurezza conforme alle politiche e agli orientamenti di sicurezza, in particolare il piano di sicurezza, le SecOP relative al sistema e la documentazione crittografica nell'ambito della procedura di accreditamento del CIS;

b) partecipare alla selezione e alla prova di misure, dispositivi e software di sicurezza tecnica specifici del sistema, per sorvegliarne l'attuazione ed assicurarne l'installazione, la configurazione e la manutenzione in modo sicuro conformemente alla relativa documentazione di sicurezza;

c) partecipare alla selezione di misure di sicurezza e dispositivi TEMPEST se richiesto nel piano di sicurezza e assicurarne l'installazione e la manutenzione in modo sicuro in collaborazione con l'autorità TEMPEST;

d) controllare l'attuazione e l'applicazione delle SecOP relative al funzionamento del sistema;

e) gestire e trattare prodotti crittografici, in collaborazione con l'autorità di distribuzione degli apparati crittografici, per assicurare la custodia adeguata del materiale crittografico e degli apparati controllati e, se richiesto, garantire la produzione di variabili crittografiche;

f) svolgere analisi, esami e verifiche di sicurezza, in particolare per elaborare le pertinenti relazioni sui rischi, come richiesto dall'autorità di accreditamento di sicurezza;

g) fornire una formazione specifica al CIS in materia di garanzia di sicurezza delle informazioni;

h) attuare e mettere in funzione misure di sicurezza specifiche del CIS.

CAPO 4

Responsabile locale della sicurezza

Articolo 11

Nomina dell'LSO

1. L'LSO e l'LSO aggiunto sono funzionari o agenti temporanei.

2. Tutti gli LSO e i loro aggiunti sono in possesso di un'autorizzazione di sicurezza valida per l'accesso alle ICUE fino al livello SECRET UE/EU SECRET e, laddove necessario, fino al livello TRÈS SECRET UE/EU TOP SECRET. L'LSO o l'LSO aggiunto ottiene l'autorizzazione di sicurezza prima della nomina.

3. Le rappresentanze della Commissione possono chiedere all'autorità di sicurezza della Commissione di derogare ai requisiti previsti ai paragrafi 1 e 2.

Articolo 12

Procedure operative di sicurezza per le zone protette

1. In ogni servizio della Commissione interessato l'LSO elabora le SecOP per ciascuna delle zone protette di cui è responsabile.

2. L'LSO provvede affinché le SecOP comprendano i seguenti requisiti:

a) soltanto i membri del personale in possesso di un'autorizzazione di sicurezza valida e di cui è accertata la necessità di accedere a documenti classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono autorizzati ad accedere senza scorta a una zona protetta durante l'orario d'ufficio;

b) l'accesso senza scorta a una zona protetta al di fuori dell'orario d'ufficio è permesso soltanto all'LSO del servizio, agli RCO della zona protetta, ai loro aggiunti e al personale autorizzato della direzione Sicurezza della direzione generale Risorse umane e sicurezza;

c) all'interno delle zone protette non sono ammessi dispositivi di registrazione e comunicazione quali telefoni mobili, computer, apparecchi fotografici o altri dispositivi intelligenti senza la previa autorizzazione dell'autorità di sicurezza della Commissione; un'eventuale deroga è richiesta in anticipo all'autorità di sicurezza della Commissione. L'LSO agisce da punto di contatto;

d) il personale interno o esterno che ha necessità di accedere a una zona protetta ma che non soddisfa i criteri previsti alla lettera a) è scortato all'interno e sottoposto in ogni momento alla sorveglianza di un membro del personale debitamente autorizzato; tutti gli accessi di questo tipo a una zona protetta sono registrati in un repertorio conservato all'ingresso della zona protetta;

e) l'LSO provvede affinché i sistemi di rilevamento delle intrusioni che controllano una zona protetta siano costantemente attivi e correttamente funzionanti e gestisce tutte le password, chiavi, PIN o altri meccanismi di accesso e di autenticazione;

f) gli allarmi in una zona protetta sono segnalati alla direzione Sicurezza della direzione generale Risorse umane e sicurezza, che provvede immediatamente a notificarli all'LSO;

g) l'LSO del servizio in cui è ubicata la zona protetta conserva traccia di ciascun intervento attuato in seguito a un allarme o a un incidente di sicurezza;

h) sono predisposte procedure per i casi di allarme o per altre situazioni di emergenza all'interno della zona protetta, tra cui l'evacuazione del personale e, se necessario, la risposta rapida da parte di una squadra di emergenza sotto la direzione dell'autorità di sicurezza della Commissione e di servizi di emergenza esterni;

i) l'LSO segnala immediatamente all'autorità di sicurezza della Commissione qualsiasi violazione della sicurezza verificatasi all'interno di una zona protetta o che interessa una zona protetta, al fine di determinare la risposta appropriata;

j) i singoli uffici e le singole sale e casseforti all'interno di una zona protetta restano chiusi a chiave ogniqualvolta siano lasciati incustoditi;

k) il personale evita di discutere di informazioni classificate nei corridoi o in altre aree comuni della zona protetta se nelle vicinanze sono presenti persone non autorizzate.

Articolo 13

Chiavi e combinazioni di sicurezza

1. L'LSO ha la responsabilità generale della corretta gestione e conservazione delle chiavi e delle combinazioni usate all'interno delle zone protette o per accedervi. Le chiavi e combinazioni sono conservate in un contenitore di sicurezza e ricevono almeno la stessa protezione riservata al materiale a cui danno accesso.

2. L'LSO tiene un registro dei contenitori di sicurezza e delle camere blindate, unitamente a un elenco aggiornato di tutti i membri del personale che possono accedervi senza scorta.

3. L'LSO tiene un registro delle chiavi dei contenitori di sicurezza e delle camere blindate, con indicazione dei membri del personale ai quali sono assegnate. Per ciascuna chiave assegnata è conservata una ricevuta che riporta l'identificativo della chiave, il destinatario e la data e ora.

4. Le chiavi e combinazioni sono assegnate unicamente al personale che ha «necessità di conoscere» e a cui è stata rilasciata la necessaria autorizzazione per l'accesso alle ICUE. L'LSO recupera la chiave laddove dette condizioni non siano più soddisfatte.

5. L'LSO conserva le chiavi di riserva e una traccia scritta di tutte le combinazioni all'interno di singole buste opache sigillate, firmate e datate, fornite dal membro del personale responsabile delle chiavi. Le buste sono conservate in un contenitore di sicurezza idoneo al livello di classifica più elevato del materiale conservato nel contenitore stesso o nella camera blindata.

6. Se al momento della modifica della combinazione o della rotazione della chiave la busta presenta segni di manomissione o danneggiamento, l'LSO considera l'evento un incidente di sicurezza e ne informa immediatamente l'autorità di sicurezza della Commissione.

7. Le combinazioni dei contenitori di sicurezza nelle zone protette sono modificate sotto la supervisione dell'LSO. Le combinazioni sono modificate almeno ogni dodici mesi e:

a) al ricevimento di un nuovo contenitore o al momento dell'installazione di una nuova serratura (in particolare le combinazioni predefinite devono essere modificate immediatamente);

b) in caso di compromissione o sospetta compromissione;

c) quando non è più necessario l'accesso di una persona in possesso della combinazione.

8. L'LSO tiene registrazione delle date delle modifiche delle combinazioni di cui al paragrafo 7.

Articolo 14

Piani di evacuazione e di distruzione di emergenza delle ICUE

1. L'LSO assiste il caposervizio nell'elaborazione dei piani di evacuazione e di distruzione di emergenza delle ICUE sulla base degli orientamenti emanati dalla direzione Sicurezza della direzione generale Risorse umane e sicurezza.

2. L'LSO provvede affinché qualsiasi attrezzatura necessaria per l'operatività dei piani previsti al paragrafo 1 sia disponibile prontamente e mantenuta in buono stato di funzionamento.

3. L'LSO esamina, insieme ai funzionari designati nei piani previsti al paragrafo 1, lo stato di preparazione dei piani almeno ogni dodici mesi e intraprende ogni azione necessaria per aggiornarli.

Articolo 15

Autorizzazioni di sicurezza

1. L'LSO tiene un registro di tutti i posti in seno al servizio per cui è necessaria un'autorizzazione di sicurezza della Commissione, e del personale che li occupa. L'obbligo di autorizzazione di sicurezza deve essere precisato nell'avviso di posto vacante nell'iter di assunzione e comunicato al candidato durante il colloquio.

2. L'LSO supervisiona ciascuna domanda di autorizzazione di sicurezza per l'accesso alle ICUE. L'LSO è il punto di contatto in seno al servizio e tiene i contatti con l'autorità di sicurezza della Commissione ai fini delle autorizzazioni di sicurezza.

3. L'LSO avvia la domanda di attivazione della procedura di autorizzazione di sicurezza per il membro del personale e provvede affinché questi restituisca prontamente all'autorità di sicurezza della Commissione il questionario compilato per l'ottenimento del nulla osta di sicurezza nazionale.

4. L'LSO provvede affinché il personale del servizio in possesso di nulla osta di sicurezza partecipi alla sessione informativa obbligatoria sulle ICUE al fine di ottenere l'autorizzazione di sicurezza.

5. L'LSO consulta periodicamente l'ufficio risorse umane del servizio per informarsi su qualsiasi cambiamento intervenuto in relazione ai posti per i quali è necessaria l'autorizzazione di sicurezza e ne informa immediatamente l'autorità di sicurezza della Commissione.

6. L'LSO informa l'autorità di sicurezza della Commissione dell'arrivo di ciascun nuovo membro del personale in possesso di nulla osta di sicurezza che è assegnato a un posto per il quale è necessaria l'autorizzazione di sicurezza.

7. L'LSO provvede affinché i membri del personale del servizio completino la procedura di rinnovo del nulla osta di sicurezza entro il termine stabilito. Il membro del personale che rifiuta di completare la procedura è obbligato a trasferirsi ad un posto per il quale l'autorizzazione di sicurezza non è necessaria.

Articolo 16

Ufficio di registrazione delle ICUE

1. Laddove il servizio gestisca un ufficio di registrazione delle ICUE, l'LSO supervisiona le attività degli RCO per quanto riguarda il trattamento delle ICUE e la conformità alle norme di sicurezza per la protezione delle ICUE.

2. L'LSO esegue i seguenti controlli almeno ogni dodici mesi e in caso di sostituzione dell'RCO o dell'RCO aggiunto:

a) controllo di un campione di documenti nell'ufficio di registrazione delle ICUE per confermarne lo status e verificare la precisione del registro dei documenti classificati;

b) controllo di un campione di ricevute e note di trasmissione per la distribuzione delle ICUE in entrata e in uscita dall'ufficio di registrazione delle ICUE;

c) controllo di un campione di certificati di distruzione.

3. Almeno una volta al mese l'LSO esegue controlli a campione del registro dei documenti classificati e dei documenti classificati ricevuti di recente per verificare la corretta registrazione dei documenti.

4. Tutti i controlli sono registrati nel log del registro dei documenti classificati.

Articolo 17

Altre responsabilità in materia di sicurezza

Le altre responsabilità dell'LSO in materia di sicurezza sono definite in una comunicazione di sicurezza riguardante in particolare la sicurezza fisica di persone, locali e altre risorse e delle informazioni.

CAPO 5

Funzionario responsabile del controllo delle registrazioni

Articolo 18

Nomina dell'RCO

1. L'RCO e l'RCO aggiunto sono funzionari o agenti temporanei.

2. Tutti gli RCO e i loro aggiunti sono in possesso di un'autorizzazione di sicurezza valida per l'accesso alle ICUE fino al livello SECRET UE/EU SECRET e, laddove necessario, fino al livello TRÈS SECRET UE/EU TOP SECRET. L'RCO o l'RCO aggiunto ottiene l'autorizzazione di sicurezza prima della nomina.

3. Le rappresentanze della Commissione possono chiedere all'autorità di sicurezza della Commissione di derogare ai requisiti previsti ai paragrafi 1 e 2.

Articolo 19

Responsabilità

1. L'RCO registra le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore a fini di sicurezza:

a) all'entrata o all'uscita da un servizio della Commissione; oppure

b) all'entrata o all'uscita da un CIS.

2. L'RCO registra tutti gli eventi del ciclo di vita di tutte le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore. L'RCO provvede inoltre affinché sia conservata registrazione di tutte le informazioni classificate di livello RESTREINT UE/EU RESTRICTED o equivalente che sono oggetto di scambio con paesi terzi e organizzazioni internazionali. A tal fine opera in coordinamento con l'ufficio di registrazione delle ICUE gestito dal segretariato generale.

3. L'RCO registra i documenti classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore nel registro dei documenti classificati e provvede affinché siano conservati in sicurezza all'interno dell'ufficio di registrazione delle ICUE.

4. L'RCO assiste il personale della Commissione nella creazione e nella trasmissione di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore.

5. In caso di ricezione di documenti classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore da altri servizi o da soggetti esterni, l'RCO provvede a che la ricevuta di consegna sia debitamente restituita all'originatore.

6. Prima di autorizzare il membro del personale ad accedere a un documento classificato detenuto dall'ufficio di registrazione delle ICUE, l'RCO verifica con l'LSO che il membro del personale sia in possesso di un'autorizzazione di sicurezza rilasciata dall'autorità di sicurezza della Commissione.

7. L'RCO registra tutte le entrate e le uscite dall'ufficio di registrazione delle ICUE di membri del personale non autorizzati ad accedervi senza scorta e li accompagna per tutta la durata della visita.

8. Quando un membro del personale preleva un documento al fine di consultarlo all'esterno dell'ufficio di registrazione delle ICUE, l'RCO provvede a che il membro del personale sia al corrente delle necessarie misure di sicurezza compensative e restituisca il documento non appena non sia più necessario. L'RCO rammenta al membro del personale di restituire il documento in tempi il più possibile brevi.

9. L'ufficio di registrazione delle ICUE rilascia il certificato di corriere quando un documento classificato è trasportato a mano fuori del paese in cui è ubicato l'ufficio di registrazione.

10. Una comunicazione di sicurezza impartisce all'RCO istruzioni particolareggiate circa la registrazione dei documenti classificati.

Articolo 20

Declassamento e declassificazione

L'RCO assiste il servizio originatore nel riesame delle ICUE registrate al fine di stabilire se il livello di classifica originario sia ancora adeguato o se sia possibile declassare o declassificare il documento.

Articolo 21

Distruzione

1. L'RCO è responsabile della distruzione con mezzo approvato delle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore, se del caso in presenza di testimoni in possesso di nulla osta di sicurezza.

2. L'RCO registra la distruzione di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore nel registro dei documenti classificati e conserva i relativi certificati di distruzione nell'ufficio di registrazione delle ICUE.

Articolo 22

Compiti aggiuntivi

1. L'RCO offre all'LSO tutta l'assistenza necessaria per lo svolgimento di attività di supervisione nell'ufficio di registrazione delle ICUE.

2. L'RCO segnala gli incidenti di sicurezza effettivi o presunti all'LSO, il quale a sua volta li segnala all'autorità di sicurezza della Commissione.

3. L'RCO dell'ufficio di registrazione delle ICUE di un servizio della Commissione che organizza una riunione classificata di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore prepara le ICUE che saranno trattate durante la riunione e si coordina con l'organizzatore della riunione affinché tutti i documenti e tutte le ricevute siano trattati in conformità delle norme applicabili.

CAPO 6

Disposizioni finali

Articolo 23

Trasparenza

La presente decisione è resa nota al personale della Commissione e a tutte le persone cui si applica ed è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 24

La presente decisione entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 7 aprile 2022

Per la Commissione
a nome della presidente
Gertrud INGESTAD
Direttrice generale
Direzione generale Risorse umane e sicurezza