

## IV

(Informazioni)

INFORMAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E  
DAGLI ORGANISMI DELL'UNIONE EUROPEA

## SERVIZIO EUROPEO PER L'AZIONE ESTERNA

DECISIONE DELL'ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA  
POLITICA DI SICUREZZA

del 19 aprile 2013

relativa alle norme di sicurezza del Servizio europeo per l'azione esterna

(2013/C 190/01)

L'ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA,

vista la decisione 2010/427/UE del Consiglio, del 26 luglio 2010, che fissa l'organizzazione e il funzionamento del Servizio europeo per l'azione esterna (SEAE) <sup>(1)</sup>,

visto il parere del Comitato di cui all'articolo 9, paragrafo 6, della decisione dell'Alto rappresentante, del 15 giugno 2011, relativa alle norme di sicurezza del Servizio europeo per l'azione esterna <sup>(2)</sup>,

visto il parere del comitato di cui all'articolo 10, paragrafo 1, della decisione 2010/427/UE del Consiglio, del 26 luglio 2010, che fissa l'organizzazione e il funzionamento del SEAE,

considerando quanto segue:

(1) In quanto organo dell'Unione europea (UE) che opera in autonomia funzionale, il SEAE deve essere dotato di norme di sicurezza, come previsto all'articolo 10, paragrafo 1, della decisione 2010/427/UE del Consiglio.

(2) L'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (in seguito, "Alto rappresentante" o "AR") deve adottare norme di sicurezza del SEAE che contemplino tutti gli aspetti della sicurezza relativi al funzionamento del SEAE affinché quest'ultimo possa gestire efficacemente i rischi per il personale posto la sua

responsabilità, per i beni materiali, le informazioni e i visitatori e assolvere l'obbligo di diligenza che gli incombe a tale riguardo.

(3) Occorre segnatamente dotare il personale posto sotto la responsabilità del SEAE, i beni materiali, compresi i sistemi di comunicazione e informazione, le informazioni e i visitatori del SEAE, di un livello di protezione comparabile alle migliori prassi applicate al Consiglio, alla Commissione e negli Stati membri e, eventualmente, nelle organizzazioni internazionali.

(4) È opportuno che le norme di sicurezza del SEAE contribuiscano all'elaborazione di un quadro generale completo e più coerente nell'UE per proteggere le informazioni classificate UE (in seguito, "ICUE"), in base alle norme di sicurezza del Consiglio dell'Unione europea (in seguito, "il Consiglio") e alle disposizioni della Commissione europea in materia di sicurezza, mantenendo la coerenza generale.

(5) Il SEAE, il Consiglio e la Commissione si impegnano ad applicare norme di sicurezza equivalenti per proteggere le ICUE.

(6) La presente decisione lascia impregiudicati gli articoli 15 e 16 del trattato sul funzionamento dell'Unione europea (TFUE) e i relativi strumenti di attuazione.

(7) È necessario definire l'organizzazione della sicurezza nel SEAE e l'attribuzione delle mansioni di sicurezza all'interno delle sue strutture.

<sup>(1)</sup> GU L 201 del 3.8.2010, pag. 30.

<sup>(2)</sup> GU C 304 del 15.10.2011, pag. 5.

- (8) L'Alto rappresentante deve, all'occorrenza, avvalersi delle competenze tecniche esistenti negli Stati membri, al Segretariato generale del Consiglio e alla Commissione.
- (9) L'Alto rappresentante deve adottare tutte le idonee misure necessarie per dare attuazione alle norme di sicurezza con il sostegno degli Stati membri, del Segretariato generale del Consiglio e della Commissione,

che contengono i sistemi di comunicazione e informazione (compresi quelli che trattano ICUE), in cui il SEAE svolge attività permanenti o temporanee.

- (e) "interessi del SEAE in materia di sicurezza": il personale posto sotto la responsabilità del SEAE, i locali, le persone a carico, i beni materiali, compresi i sistemi di comunicazione e di informazione, le informazioni e i visitatori di quest'ultimo.

HA ADOTTATO LA PRESENTE DECISIONE:

#### Articolo 1

##### Oggetto e ambito di applicazione

La presente decisione stabilisce le norme di sicurezza applicabili al Servizio europeo per l'azione esterna (in seguito, "norme di sicurezza del SEAE").

Ai sensi dell'articolo 10, paragrafo 1, della decisione 2010/427/UE del Consiglio, del 26 luglio 2010, che fissa l'organizzazione e il funzionamento del Servizio europeo per l'azione esterna, la presente decisione si applica al personale del SEAE e a tutto il personale delle delegazioni dell'Unione a prescindere dalla condizione amministrativa o dalla provenienza, e istituisce un quadro normativo generale di gestione efficace dei rischi cui sono soggetti il personale posto sotto la responsabilità del SEAE, di cui all'articolo 2, i locali, i beni materiali, le informazioni e i visitatori.

#### Articolo 2

##### Definizioni

Ai fini della presente decisione si intende per:

- (a) "personale del SEAE": i funzionari del SEAE e altri agenti, tra cui i membri dei servizi diplomatici degli Stati membri nominati agenti temporanei, gli esperti nazionali distaccati, ai sensi dell'articolo 6 della decisione 2010/427/UE del Consiglio, del 26 luglio 2010, che fissa l'organizzazione e il funzionamento del Servizio europeo per l'azione esterna.
- (b) "personale posto sotto la responsabilità del SEAE": il personale del SEAE e tutto il personale delle delegazioni dell'Unione a prescindere dalla condizione amministrativa o dalla provenienza, nonché, ai fini della presente decisione, l'Alto rappresentante e, se del caso, altro personale in servizio nei locali della sede centrale del SEAE.
- (c) "persone a carico": i familiari del personale posto sotto la responsabilità del SEAE nelle delegazioni dell'Unione che sono compresi nei rispettivi nuclei familiari come notificato al ministero degli Affari esteri dello Stato ospitante.
- (d) "locali del SEAE": tutti gli stabilimenti del SEAE, compresi gli edifici, gli uffici, le stanze o altre zone, nonché le zone

- (f) "ICUE": qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE, la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri.

Altre definizioni sono elencate negli allegati pertinenti e nell'appendice A.

#### Articolo 3

##### Obbligo di diligenza

1. Le norme di sicurezza del SEAE intendono assolvere l'obbligo di diligenza che incombe al SEAE.
2. L'obbligo di diligenza del SEAE richiede di intraprendere con debita diligenza ogni iniziativa idonea per attuare misure di sicurezza volte a prevenire danni ragionevolmente prevedibili agli interessi del SEAE in materia di sicurezza.

Esso sottende elementi che attengono sia alla sicurezza che all'incolumità delle persone, compresi quelli determinati da situazioni di emergenza o di crisi, indipendentemente dalla loro natura.

3. Considerato l'obbligo di diligenza degli Stati membri, delle istituzioni e degli organi dell'UE, e di altre parti con personale proprio presso le delegazioni dell'Unione e/o nei locali delle delegazioni dell'Unione, o considerato che tale responsabilità incombe sul SEAE quando le delegazioni dell'Unione sono ospitate nei locali delle suddette altre parti, il SEAE conclude accordi amministrativi con ciascuna delle suddette entità per definire i rispettivi ruoli e responsabilità, compiti e meccanismi di cooperazione.

#### Articolo 4

##### Sicurezza materiale e delle infrastrutture

1. Per la tutela dei suoi interessi in materia di sicurezza, il SEAE attua tutte le misure di sicurezza materiale adeguate (permanenti o temporanee), comprese le modalità di controllo dell'accesso, in tutti i suoi locali. Di tali misure si terrà conto nella progettazione e nella pianificazione di nuovi locali o prima di prenderne in locazione di esistenti.

2. Nei paesi terzi, il SEAE attuerà ogni ulteriore misura di sicurezza materiale utile, permanente o temporanea, ai fini della tutela dei propri interessi in materia di sicurezza.

A tal fine, al personale posto sotto la responsabilità del SEAE, e alle rispettive persone a carico, per ragioni di sicurezza possono essere imposti obblighi o restrizioni speciali per un periodo specifico o in zone specifiche.

3. Le misure di cui ai paragrafi 1 e 2 sono commisurate alla valutazione del rischio.

#### Articolo 5

##### Protezione delle informazioni classificate

1. La protezione delle ICUE è disciplinata dalle disposizioni di cui alla presente decisione, in particolare all'allegato A, conformemente alle quali il detentore di qualsiasi ICUE è responsabile della sua protezione.

2. Il SEAE provvede affinché l'accesso alle informazioni classificate sia consentito solo alle persone che soddisfano le condizioni di cui all'articolo 5 dell'allegato A.

3. Le condizioni alle quali gli agenti locali possono avere accesso alle ICUE sono stabilite anch'esse dall'Alto rappresentante, conformemente alle norme per la protezione delle ICUE di cui all'allegato A della presente decisione.

4. La direzione "Sicurezza" del SEAE gestisce una banca dati di sicurezza di tutto il personale posto sotto la responsabilità del SEAE e dei suoi contraenti.

5. Quando gli Stati membri introducono informazioni classificate che recano un contrassegno di classifica di sicurezza nazionale nelle strutture o nelle reti del SEAE, quest'ultimo protegge tali informazioni conformemente ai requisiti applicabili alle ICUE di livello equivalente, come indicato nelle norme applicabili ai sensi dell'allegato A della presente decisione.

6. Le zone nel SEAE, in cui sono conservate informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, o classificate ad un livello equivalente, sono costituite come zone sicure, conformemente alle norme di cui all'allegato A della presente decisione, e sono approvate dall'autorità di sicurezza del SEAE.

7. Le procedure per l'esercizio di responsabilità da parte dell'Alto rappresentante nel quadro di accordi o intese amministrative per lo scambio di ICUE con Stati terzi o organizzazioni

internazionali sono descritte negli allegati A e A VI della presente decisione.

#### Articolo 6

##### Incidenti ed emergenze in materia di sicurezza

1. Al fine di garantire una risposta tempestiva ed efficace agli incidenti riguardanti la sicurezza, il SEAE istituisce una procedura per comunicare tali incidenti ed emergenze, operativa 24 ore al giorno, 7 giorni alla settimana, competente per qualsiasi tipo di incidente o minaccia ai suoi interessi in materia di sicurezza (ad esempio, infortuni, conflitti, atti dolosi, atti criminali, rapimenti e prese d'ostaggi, emergenze sanitarie, incidenti dei sistemi di comunicazione e d'informazione, attacchi informatici, ecc.).

2. Si istituiscono canali di collegamento di emergenza tra la sede centrale del SEAE, le delegazioni dell'Unione, il Consiglio, la Commissione, i rappresentanti speciali dell'Unione europea e gli Stati membri al fine di aiutare questi ultimi nella gestione degli incidenti riguardanti la sicurezza, che coinvolgono il personale, e delle loro conseguenze, compresa la pianificazione di emergenza.

3. Tale gestione degli incidenti riguardanti la sicurezza comprende, tra l'altro:

— procedure per sostenere in maniera efficace il processo decisionale in relazione a un incidente riguardante la sicurezza che coinvolga il personale, comprese le decisioni circa l'estrazione o la sospensione di una missione; nonché

— criteri e procedure per il recupero del personale – ad esempio, in caso di scomparsa di membri del personale o di rapimenti e prese di ostaggi – tenendo conto delle particolari responsabilità a tale riguardo degli Stati membri, delle istituzioni dell'UE e del SEAE. Nel valutare la necessità di capacità specifiche per gestire, sotto questo aspetto, tali operazioni, si tiene conto delle risorse che potrebbero essere apprestate dagli Stati membri.

4. Il SEAE attua adeguate procedure amministrative per segnalare gli incidenti riguardanti la sicurezza nelle delegazioni dell'Unione. Se del caso, ne sono informati gli Stati membri, la Commissione e ogni altra autorità competente, nonché i competenti comitati per la sicurezza.

5. Le procedure per la gestione degli incidenti dovrebbero essere oggetto di esercitazioni e verifiche periodiche.

#### Articolo 7

##### Sicurezza dei sistemi di comunicazione e informazione

1. Il SEAE protegge le informazioni trattate nei sistemi di comunicazione e informazione (CIS) dalle minacce alla riservatezza, integrità, disponibilità, autenticità e non disconoscibilità.

2. L'autorità di sicurezza del SEAE, definita all'articolo 12, sezione I, paragrafo 1, approva norme, una politica e un programma in materia di sicurezza per proteggere tutti i CIS appartenenti al SEAE o da quest'ultimo gestiti.

3. Tali norme, politica e programma sono conformi e attuati in stretto coordinamento con quelli del Consiglio e della Commissione e, se del caso, con le politiche in materia di sicurezza applicate dagli Stati membri.

4. Tutti i CIS che trattano informazioni classificate sono sottoposti a una procedura di accreditamento. Il SEAE attua un sistema di gestione degli accreditamenti di sicurezza concertato con il Segretariato generale del Consiglio e la Commissione.

5. Qualora la protezione delle ICUE trattate dal SEAE sia assicurata mediante prodotti crittografici, tali prodotti sono approvati dall'autorità di approvazione degli apparati crittografici del SEAE, in base a una raccomandazione del Comitato per la sicurezza del Consiglio.

6. Ove necessario, l'autorità di sicurezza del SEAE istituisce le seguenti funzioni in materia di garanzia di sicurezza delle informazioni:

- (a) un'autorità per la garanzia di sicurezza delle informazioni;
- (b) un'autorità TEMPEST;
- (c) un'autorità di approvazione degli apparati crittografici;
- (d) un'autorità di distribuzione degli apparati crittografici.

7. Per ciascun sistema l'autorità di sicurezza del SEAE istituisce le seguenti funzioni:

- (a) un'autorità di accreditamento di sicurezza;
- (b) un'autorità operativa per la garanzia di sicurezza delle informazioni.

8. Le disposizioni di attuazione del presente articolo, per quanto riguarda la protezione delle ICUE, figurano negli allegati A e A IV.

#### Articolo 8

##### **Violazioni della sicurezza e compromissione di informazioni classificate**

1. Una violazione della sicurezza è la conseguenza di un atto o di un'omissione di una persona contrari alle norme di sicurezza contenute nella presente decisione e/o alle politiche o orientamenti in materia di sicurezza che precisano le misure

necessarie per la sua attuazione, approvate conformemente all'articolo 20, paragrafo 1.

2. La compromissione di informazioni classificate si verifica con la loro divulgazione, totale o parziale, a persone o entità non autorizzate.

3. Qualsiasi violazione o sospetta violazione della sicurezza e qualsiasi compromissione o sospetta compromissione di informazioni classificate è immediatamente riferita alla direzione "Sicurezza" del SEAE che adotta le misure del caso di cui all'allegato A.

4. Ogni persona responsabile di una violazione delle norme di sicurezza contenute nella presente decisione, o della compromissione di informazioni classificate, è passibile di sanzioni disciplinari e/o azioni legali secondo le disposizioni legislative, normative e regolamentari applicabili, come stabilito all'articolo 11, paragrafo 3, dell'allegato A.

#### Articolo 9

##### **Indagini su incidenti, violazioni e/o compromissioni della sicurezza e azioni correttive**

1. La direzione "Sicurezza" del SEAE assistita, ove opportuno, da esperti degli Stati membri e/o di altre istituzioni dell'UE e, ove necessario, previa autorizzazione del direttore esecutivo:

- (a) conduce indagini o verifiche, se del caso:
  - (i) qualora sia noto o vi siano ragionevoli motivi di ritenere che vi sia stata compromissione o perdita di informazioni classificate pertinenti al SEAE;
  - (ii) su qualsiasi violazione della sicurezza, accertata o sospetta, o su altri incidenti o minacce agli interessi del SEAE in materia di sicurezza;
- (b) attua tutte le azioni correttive che si rendano necessarie in esito alle indagini, se del caso.

2. Gli investigatori hanno accesso a tutte le informazioni necessarie per lo svolgimento di tali indagini e a tale riguardo ricevono pieno sostegno da tutti i servizi del SEAE.

Gli investigatori possono intraprendere azioni adeguate per salvaguardare l'insieme delle prove in modo commisurato alla gravità dei fatti oggetto dell'indagine.

3. Quando l'accesso alle informazioni ha per oggetto dati personali, compresi quelli contenuti nei sistemi di comunicazione e informazione, tale accesso deve avvenire in conformità del regolamento (CE) n. 45/2001.

4. Al garante europeo della protezione dei dati (GEPD) è data notifica, in conformità con il predetto regolamento, della creazione di una banca dati investigativa qualora questa contenga dati personali.

#### Articolo 10

##### Gestione del rischio di sicurezza

1. Nel definire le proprie esigenze in materia di sicurezza, il SEAE elabora una metodologia generale di valutazione dei rischi per la sicurezza in stretta collaborazione con la direzione "Sicurezza" della Commissione e, se del caso, con il servizio di sicurezza del Segretariato generale del Consiglio.

2. I rischi per gli interessi del SEAE in materia di sicurezza sono gestiti secondo una procedura. Tale procedura è volta a determinare i rischi noti per la sicurezza, a definire le misure di sicurezza per contenere tali rischi entro un livello accettabile e ad applicare misure secondo il concetto di difesa in profondità. L'efficacia di tali misure e il livello di rischio sono sottoposti a costante valutazione.

3. I ruoli, le responsabilità e i compiti stabiliti nella presente decisione non pregiudicano la responsabilità di ciascun membro del personale posto sotto la responsabilità del SEAE; in particolare, il personale dell'Unione in missione in paesi terzi deve comportarsi con buon senso e discernimento rispetto alla propria incolumità e sicurezza e rispettare tutte le norme, regolamenti, procedure e istruzioni di sicurezza applicabili.

4. Il SEAE prende tutte le misure del caso per proteggere i propri interessi in materia di sicurezza e per prevenire danni ragionevolmente prevedibili.

5. Le misure di sicurezza del SEAE per proteggere le ICUE nel corso del loro ciclo di vita sono commisurate in particolare alla rispettiva classifica di sicurezza, alla forma e al volume delle informazioni o dei materiali, all'ubicazione e alla costruzione delle strutture in cui sono conservate le ICUE e alla valutazione, anche a livello locale, della minaccia di attività dolose e/o criminali, compreso lo spionaggio, il sabotaggio e il terrorismo.

#### Articolo 11

##### Formazione e sensibilizzazione alla sicurezza

1. L'autorità di sicurezza del SEAE provvede a elaborare e attuare programmi di formazione e sensibilizzazione alla sicurezza e a far impartire ai membri del personale posto sotto la responsabilità del SEAE nonché, se del caso, alle rispettive persone a carico, le necessarie istruzioni sulla sensibilizzazione e la formazione proporzionate ai rischi esistenti nel luogo di lavoro o di residenza.

2. Prima che gli sia accordato l'accesso alle ICUE, e successivamente ad intervalli regolari, il personale è informato e

riconosce le proprie responsabilità in materia di protezione delle ICUE, conformemente alle norme di cui all'articolo 5.

#### Articolo 12

##### Organizzazione della sicurezza nel SEAE

###### Sezione 1

##### Disposizioni generali

1. Il direttore esecutivo è l'autorità di sicurezza del SEAE. In tale veste, il direttore esecutivo provvede affinché:

- (a) le misure di sicurezza siano coordinate ove necessario con le competenti autorità degli Stati membri, il Segretariato generale del Consiglio e la Commissione e, se del caso, di Stati terzi o organizzazioni internazionali, su tutti gli aspetti della sicurezza pertinenti alle attività del SEAE, compresa la natura delle minacce agli interessi del SEAE in materia di sicurezza e i mezzi di protezione da tali minacce;
- (b) si tenga pienamente conto degli aspetti della sicurezza fin dall'avvio di tutte le attività del SEAE;
- (c) l'accesso alle informazioni classificate sia consentito solo alle persone che soddisfano le condizioni di cui all'articolo 5 dell'allegato A;
- (d) sia istituito un sistema di registrazione affinché le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore siano trattate conformemente alla presente decisione nell'ambito del SEAE e quando rese agli Stati membri, a istituzioni, organi o agenzie dell'UE o ad altri destinatari autorizzati; si tenga una registrazione separata di tutte le ICUE trasmesse dal SEAE a Stati terzi e organizzazioni internazionali e di tutte le informazioni classificate ricevute da paesi terzi o da organizzazioni internazionali;
- (e) siano effettuate le ispezioni di sicurezza di cui all'articolo 15;
- (f) siano condotte indagini su violazioni di sicurezza, accertate o sospette, comprese compromissioni o perdite, accertate o sospette, di informazioni classificate detenute o originate dal SEAE e sia chiesto alle competenti autorità di sicurezza di partecipare a tali indagini;
- (g) per fornire una risposta tempestiva ed efficace agli incidenti in materia di sicurezza, siano stabiliti idonei piani e meccanismi di gestione degli incidenti e delle relative conseguenze;
- (h) siano adottate adeguate misure in caso di inosservanza della presente decisione da parte di singole persone;

(i) siano predisposte idonee misure materiali e organizzative a protezione degli interessi del SEAE in materia di sicurezza.

A questo proposito, consultandosi con il Segretario generale esecutivo, il direttore esecutivo:

— fissa, di concerto con la Commissione, la categoria di sicurezza delle delegazioni,

— decide, previa consultazione con l'AR, quando il personale delle delegazioni debba essere evacuato, qualora la situazione lo richieda sotto il profilo della sicurezza,

— decide, ove opportuno, sulle misure applicabili alla protezione delle persone a carico, tenendo conto degli accordi con le istituzioni dell'UE di cui all'articolo 3, paragrafo 3,

— approva la politica in materia di comunicazione crittografata, in particolare il programma di installazione dei prodotti e del meccanismo di crittografia.

2. In questo compito il direttore esecutivo è assistito dal direttore generale per le Finanze e gli affari amministrativi, dal capo della direzione "Sicurezza" del SEAE e, se del caso, dal direttore generale per la risposta alle crisi e coordinatore operativo.

3. A tale riguardo, e secondo il caso, il direttore esecutivo, in quanto autorità di sicurezza del SEAE, può delegare compiti.

4. Ciascun responsabile di dipartimento/divisione è responsabile dell'attuazione delle norme in materia di protezione delle ICUE all'interno del proprio dipartimento/divisione.

Ferma restando la sua responsabilità, come indicato sopra, il responsabile di ciascun dipartimento/divisione designa il personale da assegnare alla funzione di coordinatore dipartimentale della sicurezza cui sono attribuite risorse commisurate alla quantità di ICUE trattate da quel dipartimento/divisione.

I coordinatori dipartimentali della sicurezza, quando e se del caso, assistono e sostengono il proprio responsabile di dipartimento/divisione nell'espletamento dei compiti connessi alla sicurezza, quali:

(a) elaborare misure di sicurezza supplementari adeguate alle specifiche esigenze del dipartimento/divisione;

(b) tenere riunioni informative periodiche in materia di sicurezza con i membri del proprio dipartimento/divisione;

(c) assicurare il rispetto del principio della necessità di conoscere nel proprio dipartimento/divisione;

(d) mantenere aggiornato un elenco di codici e chiavi di sicurezza;

(e) mantenere procedure di sicurezza e misure di sicurezza;

(f) segnalare ogni violazione della sicurezza e/o compromissione di ICUE sia al proprio direttore che alla direzione "Sicurezza";

(g) tenere riunioni di debriefing per il personale che cessa l'incarico presso il SEAE;

(h) trasmettere periodicamente per via gerarchica relazioni sullo stato della sicurezza nel dipartimento/divisione;

(i) mantenere un collegamento con la direzione "Sicurezza" del SEAE sulle questioni in materia di sicurezza.

Qualsiasi attività o questione che possa avere un impatto sulla sicurezza è tempestivamente notificata alla direzione "Sicurezza" del SEAE.

5. Ogni capo di delegazione dell'Unione è responsabile dell'attuazione di tutte le misure attinenti alla sicurezza della delegazione dell'Unione.

## Sezione 2

### La direzione "Sicurezza" del SEAE

1. Il SEAE dispone di una direzione "Sicurezza". Essa provvede a:

(a) gestire, coordinare, controllare e/o attuare tutte le misure di sicurezza in tutti i locali sotto la responsabilità del SEAE presso la sede centrale, nell'Unione europea e negli Stati terzi;

(b) garantire coerenza e compatibilità con la presente decisione e con le disposizioni di attuazione di qualsiasi attività che possa avere un impatto sulla protezione degli interessi del SEAE in materia di sicurezza;

(c) porsi come principale consigliere dell'AR, del Segretario generale esecutivo e del direttore esecutivo su tutte le questioni relative alla sicurezza;

(d) farsi assistere dai servizi competenti degli Stati membri conformemente all'articolo 10, paragrafo 3, della decisione 2010/427/UE del Consiglio che fissa l'organizzazione e il funzionamento del SEAE;

(e) sostenere le attività dell'autorità di accreditamento di sicurezza del SEAE effettuando valutazioni della sicurezza materiale dell'ambiente di sicurezza generale/ambiente di sicurezza locale dei sistemi di comunicazione e informazione che trattano ICUE e dei locali da autorizzare per il trattamento e la conservazione di ICUE.

2. Il Capo della direzione "Sicurezza" del SEAE è responsabile delle seguenti attività:

(a) garantire la protezione generale degli interessi del SEAE in materia di sicurezza;

(b) elaborare, verificare e aggiornare le norme di sicurezza e coordinare le misure di sicurezza con le autorità competenti degli Stati membri e, se del caso, con le autorità competenti di Stati terzi e organizzazioni internazionali che hanno concluso con l'UE accordi e/o intese in materia di sicurezza;

(c) sostenere i lavori del Comitato per la sicurezza del SEAE, come stabilito all'articolo 14, paragrafo 1, della presente decisione;

(d) mantenere, se del caso, un collegamento in materia di sicurezza con partner o autorità diversi da quelli di cui alla lettera b);

(e) ordinare secondo priorità e formulare proposte per la gestione del bilancio per la sicurezza nella sede centrale e nelle delegazioni dell'Unione.

3. Il Capo della direzione "Sicurezza" del SEAE:

(a) provvede affinché le violazioni e le compromissioni della sicurezza siano registrate, e siano avviate e intraprese indagini se e quando necessario;

(b) si riunisce periodicamente, e ogniqualvolta necessario, con il direttore della sicurezza del Segretariato generale del Consiglio e il direttore della direzione "Sicurezza" della Commissione per discutere argomenti di interesse comune.

4. La direzione "Sicurezza" del SEAE prende contatto e mantiene una stretta cooperazione con:

— i servizi incaricati della sicurezza presso i ministeri degli Affari esteri degli Stati membri;

— le autorità di sicurezza nazionali (NSA) e/o le altre autorità di sicurezza competenti degli Stati membri, al fine di sollecitarne l'assistenza per quanto riguarda le informazioni di cui ha necessità ai fini della valutazione dei rischi e delle minacce che il SEAE, il suo personale, attività, beni e risorse e informazioni classificate possano trovarsi ad affrontare nella abituale sede di attività;

— le autorità di sicurezza competenti degli Stati membri o dei paesi ospitanti sul territorio dei quali il SEAE eserciti la sua attività, in relazione a qualsiasi questione inerente alla protezione del suo personale, attività, beni e risorse, e informazioni classificate, fintantoché questi si trovino nel loro territorio;

— il servizio di sicurezza del Segretariato generale del Consiglio e la direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione e, se del caso, i servizi di sicurezza delle altre istituzioni, organismi e agenzie dell'UE;

— i servizi di sicurezza di Stati terzi o organizzazioni internazionali al fine di ogni utile coordinamento, e

— le NSA degli Stati membri, in merito a qualsiasi questione relativa alla protezione delle ICUE.

### Sezione 3

#### Delegazioni dell'Unione

1. Ogni capo delegazione dell'Unione è responsabile dell'attuazione e della gestione a livello locale di tutte le misure per la protezione degli interessi del SEAE in materia di sicurezza all'interno dei locali e nell'ambito delle competenze della delegazione dell'Unione.

A questo scopo, di concerto con le competenti autorità dello Stato ospitante, egli adotterà, se necessario, tutte le misure ragionevolmente praticabili per garantire che siano attuate adeguate misure materiali e organizzative.

Se del caso, il capo delegazione elabora procedure di sicurezza per la protezione delle persone a carico ai sensi dell'articolo 2, lettera c), tenendo conto di qualsiasi accordo amministrativo, di cui all'articolo 3, paragrafo 3. Il capo delegazione presenta ogni anno una relazione su tutte le questioni attinenti alla sicurezza di sua competenza al capo della direzione "Sicurezza" del SEAE.

È assistito in queste mansioni dalla direzione "Sicurezza" del SEAE, dal personale del SEAE della delegazione che svolge specifici compiti e funzioni nel settore della sicurezza e da personale di sicurezza assegnato laddove sia necessario.

2. Inoltre, il capo delegazione:

— definisce dettagliati piani di sicurezza e di emergenza per la delegazione, sulla base di generiche procedure operative standard;

— attua un efficace sistema di gestione, 24 ore su 24, 7 giorni su 7, degli incidenti e delle emergenze riguardanti la sicurezza nell'ambito delle attività della delegazione;

- garantisce che tutto il personale della delegazione abbia una copertura assicurativa che tenga conto delle condizioni esistenti nella zona;
- garantisce che la sicurezza sia ricompresa nella formazione iniziale della delegazione dell'Unione da impartire a tutto il personale della stessa, prima o al momento dell'arrivo nella delegazione; nonché
- provvede all'attuazione di tutte le raccomandazioni formulate sulla base di valutazioni della sicurezza e trasmette periodiche relazioni scritte sulla loro attuazione e su altre questioni in materia di sicurezza all'autorità di sicurezza del SEAE.

3. Pur mantenendo la responsabilità di salvaguardare la gestione della sicurezza nonché di garantire la resilienza complessiva, il capo delegazione può delegare l'esecuzione dei suoi compiti in materia di sicurezza al coordinatore della sicurezza della delegazione nella persona del vice capo delegazione o, nel caso in cui questi non sia stato nominato, ad una figura alternativa adeguata.

In particolare, al coordinatore della sicurezza della delegazione possono essere assegnate le seguenti funzioni:

- mantenere i contatti con le competenti autorità del paese ospitante e le competenti controparti nelle ambasciate e missioni diplomatiche degli Stati membri in merito alle questioni di sicurezza;
- attuare adeguate procedure di gestione della sicurezza in funzione degli interessi del SEAE in materia di sicurezza, compresa la protezione delle ICUE;
- informare i membri del personale sulle norme di sicurezza che sono loro applicabili, nonché sui rischi specifici del paese ospitante;
- inoltrare richieste alla direzione "Sicurezza" del SEAE per i posti che necessitano di un nulla osta di sicurezza personale (PSC) e
- tenere il capo delegazione, il responsabile regionale della sicurezza e la direzione "Sicurezza" del SEAE costantemente informati in merito a incidenti o sviluppi nella zona che pregiudicano la protezione degli interessi del SEAE in materia di sicurezza.

4. Il capo delegazione può delegare mansioni di sicurezza di natura amministrativa o tecnica al capo dell'amministrazione e ad altri membri del personale della delegazione.

5. La delegazione dell'Unione è assistita da un responsabile regionale della sicurezza. Presso le delegazioni i responsabili regionali della sicurezza svolgono le funzioni di seguito definite nell'ambito di ciascuna delle rispettive aree geografiche di competenza.

In determinate circostanze, ove lo richieda la situazione contingente della sicurezza, un responsabile regionale della sicurezza può essere assegnato in servizio permanente a una delegazione specifica.

Il responsabile regionale della sicurezza può essere tenuto a trasferirsi in un'area diversa da quella di competenza, compresa la sede centrale di Bruxelles, o persino ad assumere un incarico permanente in funzione della situazione della sicurezza in qualunque paese, secondo quanto richiesto dalla direzione "Sicurezza" del SEAE.

6. I responsabili regionali della sicurezza sono posti sotto il controllo gerarchico diretto della direzione "Sicurezza" del SEAE ma sotto il diretto controllo funzionale e amministrativo del capo delegazione. Assistono il capo delegazione e il personale della delegazione nell'organizzazione e nell'attuazione di tutte le misure materiali, organizzative e procedurali relative alla sicurezza di tutti i membri del personale della delegazione, a prescindere dalla loro provenienza amministrativa.

7. I responsabili regionali della sicurezza forniscono al capo delegazione e al personale della delegazione consulenza e sostegno. Ove appropriato, in particolare qualora in servizio permanente, il responsabile regionale della sicurezza può assistere una delegazione dell'Unione nella gestione e attuazione della sicurezza, compresa la preparazione di contratti per la sicurezza, la gestione degli accreditamenti e dei nulla osta di sicurezza.

#### Articolo 13

##### Operazioni PSDC e rappresentanti speciali dell'UE

La direzione "Sicurezza" del SEAE assiste e consiglia il direttore della direzione per la gestione delle crisi e la pianificazione (CMPD), il direttore generale dello Stato maggiore dell'UE (EUMS), il comandante civile delle operazioni a capo della capacità civile di pianificazione e condotta (CPCC) e i comandanti delle operazioni militari dell'UE su aspetti relativi alla sicurezza delle operazioni PSDC, e i rappresentanti speciali dell'UE su aspetti della sicurezza relativi al loro mandato, che sono complementari alle specifiche disposizioni esistenti al riguardo nelle politiche adottate in materia dal Consiglio.

#### Articolo 14

##### Il Comitato per la sicurezza del SEAE

1. È istituito un Comitato per la sicurezza del SEAE.

È presieduto dal direttore esecutivo, o da un delegato designato, e si riunisce secondo le istruzioni del presidente o a richiesta di uno dei suoi membri. La direzione "Sicurezza" del SEAE sostiene il presidente in questa funzione e fornisce assistenza amministrativa, se necessario, ai lavori del Comitato.

2. Il Comitato per la sicurezza del SEAE è composto da rappresentanti:

- di ciascuno Stato membro;
- del servizio di sicurezza del Segretariato generale del Consiglio;
- della direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione.

La delegazione di uno Stato membro presso il Comitato per la sicurezza del SEAE può essere composta da membri:

- dell'autorità di sicurezza nazionale (NSA) e/o dell'autorità di sicurezza designata (DSA);
- dei servizi incaricati della sicurezza presso i ministeri degli Affari esteri.

3. I rappresentanti presso il Comitato possono farsi accompagnare e consigliare da esperti, se lo ritengono necessario. Possono essere invitati a partecipare rappresentanti di altre istituzioni, agenzie o organismi dell'UE quando vi si discutono questioni attinenti alla loro sicurezza.

4. Fatto salvo il disposto del paragrafo 5, il Comitato per la sicurezza del SEAE assiste il SEAE, mediante consultazioni, su tutte le questioni di sicurezza rilevanti per le attività del SEAE, per la sede centrale e le delegazioni dell'Unione.

In particolare, fatte salve le disposizioni di cui al paragrafo 5, il Comitato per la sicurezza del SEAE:

(a) è consultato relativamente a:

- politiche, orientamenti, concezioni o metodologie in materia di sicurezza, in particolare per quanto riguarda la protezione delle informazioni classificate e i provvedimenti da adottare in caso di mancato rispetto delle norme di sicurezza da parte del personale SEAE,
- aspetti tecnici della sicurezza che possano influenzare la decisione dell'AR di presentare una raccomandazione al Consiglio per l'avvio di negoziati volti a conseguire accordi sulla sicurezza delle informazioni di cui all'articolo 10, paragrafo 1, lettera a) dell'allegato A,
- eventuali modifiche alla presente decisione;

(b) può essere consultato o informato, ove opportuno, su questioni attinenti alla sicurezza del personale e dei beni entro la sede centrale del SEAE e nelle delegazioni dell'Unione, fatte salve le disposizioni dell'articolo 3, paragrafo 3;

(c) è informato di qualsiasi compromissione o perdita di ICUE che si verifichi nel SEAE.

5. Eventuali modifiche alle norme relative alla protezione delle ICUE contenute nella presente decisione e nell'allegato A richiedono il parere favorevole unanime degli Stati membri rappresentati nel Comitato per la sicurezza del SEAE. Tale parere è altresì richiesto prima di:

- avviare negoziati volti a concludere intese amministrative di cui all'articolo 10, paragrafo 1, lettera b), dell'allegato A;
- comunicare informazioni classificate nelle circostanze eccezionali di cui ai paragrafi 9, 11 e 12 dell'allegato A VI;
- assumere la responsabilità di originatore delle informazioni nelle circostanze di cui all'articolo 10, paragrafo 4, ultima frase, dell'allegato A.

La condizione del parere favorevole unanime, se necessaria, si intende soddisfatta se durante i lavori del Comitato le delegazioni degli Stati membri non hanno formulato obiezioni.

6. Il Comitato per la sicurezza del SEAE tiene in debito conto le politiche e gli orientamenti in materia di sicurezza in vigore al Consiglio e alla Commissione.

7. Il Comitato per la sicurezza del SEAE riceve l'elenco delle ispezioni annuali del SEAE e i rapporti di ispezione, una volta ultimati.

8. Organizzazione delle riunioni:

- Il Comitato per la sicurezza del SEAE si riunisce almeno due volte l'anno. Riunioni ulteriori, nella sua composizione plenaria o in quella di sicurezza dell'NSA/DSA o del ministero degli Affari esteri, possono essere fissate dal presidente o richieste dai membri del Comitato.
- Il Comitato per la sicurezza del SEAE organizza le sue attività in modo da essere in grado di formulare raccomandazioni su questioni specifiche in materia di sicurezza. Può istituire altre sotto-sezioni di esperti ove necessario. Esso redige il mandato di tali sotto-sezioni e ne riceve le relazioni di attività.
- La direzione "Sicurezza" del SEAE è responsabile della preparazione dei temi di discussione. Il presidente stabilisce l'ordine del giorno provvisorio di ogni riunione. I membri del Comitato possono proporre ulteriori temi di discussione.

*Articolo 15***Ispezioni di sicurezza**

1. L'autorità di sicurezza del SEAE assicura che siano effettuate ispezioni di sicurezza periodiche presso la sede centrale del SEAE e nelle delegazioni dell'Unione per valutare l'adeguatezza delle misure di sicurezza e verificarne la conformità alla presente decisione. La direzione "Sicurezza" del SEAE può designare, se del caso, esperti a partecipare alle ispezioni di sicurezza nelle agenzie e negli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE.

2. Le ispezioni di sicurezza del SEAE si svolgono sotto l'autorità della direzione "Sicurezza" del SEAE e, se del caso, con il sostegno di esperti in materia di sicurezza che rappresentano altre istituzioni o Stati membri dell'UE, in particolare nell'ambito degli accordi di cui all'articolo 3, paragrafo 3.

3. Se necessario, il SEAE può avvalersi delle competenze tecniche esistenti negli Stati membri, al Segretariato generale del Consiglio e alla Commissione.

Se necessario, alle ispezioni di sicurezza della delegazione dell'Unione possono essere invitati a partecipare gli esperti in materia di sicurezza presso le missioni degli Stati membri in Stati terzi e/o i rappresentanti dei servizi di sicurezza diplomatici degli Stati membri.

4. Le disposizioni di attuazione del presente articolo, per quanto riguarda la protezione delle ICUE, sono riportate nell'allegato A III.

*Articolo 16***Visite di valutazione**

Sono organizzate visite di valutazione per accertare l'efficacia delle misure di sicurezza poste in essere in uno Stato terzo o in un'organizzazione internazionale al fine di proteggere le ICUE scambiate nell'ambito di un'intesa amministrativa di cui all'articolo 10, paragrafo 1, lettera b), dell'allegato A.

La direzione "Sicurezza" del SEAE può designare esperti a partecipare alle visite di valutazione in Stati terzi o in organizzazioni internazionali con cui l'UE abbia concluso un accordo sulla sicurezza delle informazioni di cui all'articolo 10, paragrafo 1, lettera a), dell'allegato A.

*Articolo 17***Pianificazione della continuità operativa**

La direzione "Sicurezza" del SEAE assiste il direttore esecutivo nella gestione degli aspetti relativi alla sicurezza delle procedure di continuità operativa del SEAE nel quadro della pianificazione complessiva della continuità operativa del SEAE.

*Articolo 18***Consigli di viaggio per le missioni al di fuori dell'UE**

La direzione "Sicurezza" del SEAE assicura la disponibilità di consigli di viaggio al personale posto sotto la responsabilità del SEAE che effettua missioni al di fuori dell'UE attingendo alle risorse di tutti i servizi competenti del SEAE, in particolare la sala situazione dell'UE (SITROOM), il Centro dell'UE di analisi dell'intelligence (INTCEN), i dipartimenti geografici e le delegazioni dell'Unione.

La direzione "Sicurezza" del SEAE fornisce, su richiesta, e in base alle risorse di cui sopra, specifici consigli di viaggio al personale posto sotto la responsabilità del SEAE che effettua missioni in Stati terzi con un livello di rischio elevato o aumentato.

*Articolo 19***Salute e sicurezza**

Le norme di sicurezza del SEAE integrano le norme del SEAE per la tutela della salute e della sicurezza adottate dall'Alto rappresentante.

*Articolo 20***Attuazione e riesame**

1. L'autorità di sicurezza del SEAE, previa consultazione del Comitato per la sicurezza del SEAE ove opportuno, approva le politiche o gli orientamenti di sicurezza che esplicitano le misure necessarie per mettere in pratica dette norme nel SEAE e per dotarsi delle capacità necessarie per coprire tutti gli aspetti della sicurezza, in stretta cooperazione con le autorità di sicurezza competenti degli Stati membri e con il sostegno dei servizi competenti delle istituzioni UE.

2. Ai sensi dell'articolo 4, paragrafo 5, della decisione 2010/427/UE del Consiglio, del 26 luglio 2010, che fissa l'organizzazione e il funzionamento del Servizio europeo per l'azione esterna, possono trovare applicazione disposizioni transitorie attraverso accordi a livello di servizi con i servizi competenti del Segretariato generale del Consiglio e della Commissione.

3. Nell'applicazione della presente decisione l'AR assicura la coerenza generale e procede a una revisione periodica delle norme di sicurezza.

4. Le norme di sicurezza del SEAE devono essere attuate in stretta collaborazione con le autorità di sicurezza competenti degli Stati membri, con il servizio di sicurezza del Segretariato generale del Consiglio e con la direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione.

5. Il SEAE provvede affinché tutti gli aspetti del processo di sicurezza siano presi in considerazione nell'ambito del proprio sistema di risposta alle crisi.

6. Il direttore esecutivo, in quanto autorità di sicurezza, e il Capo della direzione "Sicurezza" del SEAE assicurano l'attuazione della presente decisione.

*Articolo 21*

**Sostituzione di precedenti decisioni**

1. La presente decisione abroga e sostituisce la decisione dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 15 giugno 2011 relativa alle norme di sicurezza del Servizio europeo per l'azione esterna <sup>(1)</sup>.

2. La presente decisione abroga la decisione dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 23 febbraio 2011 sulla designazione e i compiti dell'autorità delegata di sicurezza del Servizio europeo per l'azione esterna.

*Articolo 22*

**Disposizioni finali**

La presente decisione entra in vigore alla data della firma.

Essa è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Le autorità competenti del SEAE danno debita e tempestiva comunicazione a tutto il personale che rientra nel campo di applicazione della presente decisione e dei suoi allegati, del contenuto, dell'entrata in vigore e di ogni modifica ad essi apportata successivamente.

Fatto a Bruxelles, il 19 aprile 2013

*L'Alto rappresentante*  
C. ASHTON

---

<sup>(1)</sup> GU C 304 del 15.10.2011, pag. 5.

## ALLEGATO A

## PRINCIPI E NORME PER LA PROTEZIONE DELLE ICUE

## Articolo 1

**Oggetto, ambito di applicazione e definizioni**

1. Il presente allegato stabilisce i principi fondamentali e le norme minime di sicurezza per proteggere le ICUE.
2. Tali principi fondamentali e norme minime di sicurezza si applicano al SEAE e al personale sotto la sua responsabilità come indicato e definito rispettivamente agli articoli 1 e 2 della presente decisione.

## Articolo 2

**Definizione delle ICUE, delle classifiche e dei contrassegni di sicurezza**

1. Per "informazioni classificate UE" (ICUE) si intende qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE, la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri.
2. Le ICUE sono classificate ad uno dei seguenti livelli:
  - (a) TRÈS SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri.
  - (b) SECRET UE/EU SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.
  - (c) CONFIDENTIEL UE/EU CONFIDENTIAL: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.
  - (d) RESTREINT UE/EU RESTRICTED: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri.
3. Le ICUE recano un contrassegno di classifica di sicurezza conformemente al paragrafo 2. Possono recare contrassegni supplementari intesi a designare il settore di attività cui si riferiscono, identificare l'originatore, limitare la distribuzione, restringere l'uso o indicare la divulgabilità.

## Articolo 3

**Gestione delle classifiche**

1. Il SEAE garantisce che le ICUE siano adeguatamente classificate, chiaramente identificate quali informazioni classificate e conservino il loro livello di classifica solo per il tempo necessario.
2. Le ICUE sono declassate o declassificate e i contrassegni di cui all'articolo 2, paragrafo 3, sono modificati o rimossi unicamente previo consenso scritto dell'originatore.
3. L'autorità di sicurezza del SEAE, previa consultazione del Comitato per la sicurezza del SEAE conformemente all'articolo 14, paragrafo 5, della presente decisione, approva una politica di sicurezza sulla creazione di ICUE che comprende una guida pratica per la classificazione.

## Articolo 4

**Protezione delle informazioni classificate**

1. Le ICUE sono protette conformemente alla presente decisione.
2. Il detentore di ICUE è responsabile della loro protezione conformemente alla presente decisione.

3. Quando gli Stati membri introducono informazioni classificate che recano un contrassegno di classifica di sicurezza nazionale nelle strutture o nelle reti del SEAE, quest'ultimo protegge tali informazioni conformemente ai requisiti applicabili alle ICUE di livello equivalente come indicato nella tabella di equivalenza delle classifiche di sicurezza di cui all'appendice B della decisione 2011/292/UE del Consiglio, del 31 marzo 2011, sulle norme di sicurezza per la protezione delle informazioni classificate UE.

Il SEAE stabilisce procedure adeguate per conservare un'accurata documentazione in merito all'originatore:

- delle informazioni classificate che riceve; nonché
- del materiale di base incluso nelle informazioni classificate originate dal SEAE.

Il Comitato per la sicurezza del SEAE è informato in merito a tali procedure.

4. Considerevoli quantitativi di ICUE o una compilazione di esse possono richiedere un livello di protezione corrispondente a una classifica più elevata di quella dei loro componenti.

#### Articolo 5

##### **Sicurezza del personale che tratta informazioni classificate UE**

1. Per "sicurezza del personale" si intende l'applicazione di misure volte a garantire che l'accesso alle ICUE sia consentito solo alle persone che:

- hanno necessità di conoscere;
- per l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, hanno ottenuto il nulla osta di sicurezza del livello adatto o sono in altro modo debitamente autorizzate in virtù delle loro funzioni secondo le disposizioni legislative e regolamentari nazionali; nonché
- sono state informate delle proprie responsabilità in materia.

2. Le procedure per il nulla osta di sicurezza personale (PSC) determinano se una persona, in considerazione della sua lealtà, onestà e affidabilità, possa essere autorizzata ad accedere alle ICUE.

3. Prima che sia loro accordato l'accesso a ICUE e, successivamente, ad intervalli regolari, tutte le persone sono informate e riconoscono per iscritto le proprie responsabilità in materia di protezione delle ICUE conformemente alla presente decisione.

4. Le disposizioni di attuazione del presente articolo figurano nell'allegato A I.

#### Articolo 6

##### **Sicurezza materiale delle informazioni classificate UE**

1. Per "sicurezza materiale" si intende l'applicazione di misure di protezione materiali e tecniche volte ad impedire l'accesso non autorizzato alle ICUE.

2. Le misure di sicurezza materiale sono intese ad impedire ad intrusi l'ingresso fraudolento o con la forza, a scoraggiare, ostacolare e scoprire azioni non autorizzate e a consentire la differenziazione del personale per quanto riguarda l'accesso alle ICUE in base al principio della necessità di conoscere. Le misure in questione sono determinate sulla base di una procedura di gestione del rischio.

3. Le misure di sicurezza materiale sono attuate per tutti i locali, gli edifici, gli uffici, le stanze o altre zone in cui le ICUE sono trattate o conservate, comprese le zone che contengono i sistemi di comunicazione e informazione definiti all'articolo 8, paragrafo 2.

4. Le zone in cui sono conservate ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono costituite come zone sicure conformemente all'allegato A II e approvate dall'autorità di sicurezza del SEAE.

5. Per proteggere le ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore si usano solo attrezzature o dispositivi approvati.
6. Le disposizioni di attuazione del presente articolo figurano nell'allegato A II.

#### Articolo 7

##### **Gestione delle informazioni classificate**

1. Per "gestione delle informazioni classificate" si intende l'applicazione delle misure amministrative intese a controllare le ICUE per tutto il loro ciclo di vita al fine di integrare le misure previste agli articoli 5, 6 e 8 e in tal modo contribuire a scoraggiare, scoprire e porre rimedio ai casi di compromissione o perdita intenzionale o accidentale di tali informazioni. Dette misure riguardano in particolare la creazione, la registrazione, la riproduzione, la traduzione, il trasporto, il trattamento, la conservazione e la distruzione di ICUE.
2. Le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono registrate a fini di sicurezza prima della diffusione e all'atto della ricezione. Le autorità competenti presso il SEAE istituiscono un sistema di registrazione a tal fine. Le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET sono registrate in uffici di registrazione dedicati.
3. I servizi e i locali in cui sono trattate o conservate ICUE sono sottoposti a ispezioni periodiche da parte dell'autorità di sicurezza del SEAE.
4. Le ICUE sono veicolate tra i servizi e i locali al di fuori delle zone oggetto di protezione materiale secondo le modalità seguenti:
  - (a) di norma, le ICUE sono trasmesse con mezzi elettronici protetti mediante prodotti crittografici approvati conformemente all'articolo 7, paragrafo 5, della decisione e in funzione di procedure operative di sicurezza (SecOp) definite esplicitamente;
  - (b) qualora non siano usati i mezzi di cui alla lettera a), le ICUE sono trasportate:
    - (i) su supporti elettronici (ad esempio chiave USB, CD, disco rigido) protetti mediante prodotti crittografici approvati conformemente all'articolo 7, paragrafo 5 della presente decisione; oppure
    - (ii) in tutti gli altri casi, secondo quanto prescritto dall'autorità di sicurezza del SEAE, conformemente alle pertinenti misure di protezione di cui all'allegato A III, sezione V.
5. Le disposizioni di attuazione del presente articolo figurano nell'allegato A III.

#### Articolo 8

##### **Protezione delle ICUE trattate nei sistemi di comunicazione e informazione**

1. Per "garanzia di sicurezza delle informazioni (IA) nel campo dei sistemi di comunicazione e informazione" si intende la fiducia nel fatto che tali sistemi proteggeranno le informazioni che trattano e funzioneranno nel modo dovuto e a tempo debito sotto il controllo degli utenti legittimi. Una IA efficace garantisce gli adeguati livelli di riservatezza, integrità, disponibilità, non disconoscibilità e autenticità. L'IA si basa su una procedura di gestione del rischio.
2. Per "sistema di comunicazione e informazione" (CIS) si intende ogni sistema che consente il trattamento delle informazioni in forma elettronica. Un sistema di comunicazione e informazione comprende l'insieme delle risorse necessarie al suo funzionamento, ivi compresi l'infrastruttura, l'organizzazione, il personale e le risorse dell'informazione. Il presente allegato si applica a tutti i CIS del SEAE che trattano ICUE.
3. I CIS trattano le ICUE conformemente al concetto di IA.
4. Tutti i CIS che trattano ICUE sono sottoposti a una procedura di accreditamento. L'accreditamento ha lo scopo di ottenere la garanzia che sono state messe in atto tutte le misure di sicurezza adeguate e che si è raggiunto un livello sufficiente di protezione delle ICUE e del CIS, conformemente alla presente decisione. La dichiarazione di accreditamento determina il livello di classifica più elevato delle informazioni che può essere trattato in un CIS nonché i termini e le condizioni ivi associati.

5. I CIS che trattano informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore sono protetti in modo tale che le informazioni non possano essere compromesse da radiazioni elettromagnetiche non intenzionali ("misure di sicurezza TEMPEST").
6. Qualora la protezione delle ICUE sia assicurata mediante prodotti crittografici, tali prodotti sono approvati secondo l'articolo 7, paragrafo 5, della presente decisione.
7. Per la trasmissione di ICUE con mezzi elettronici si usano prodotti crittografici approvati. In deroga a tale requisito, si possono applicare procedure specifiche in particolari situazioni di emergenza o in configurazioni tecniche specifiche di cui all'allegato A IV.
8. A norma dell'articolo 7, paragrafo 6, della presente decisione, ove necessario sono stabilite le seguenti funzioni relative alla IA:
  - (a) un'autorità IA (IAA);
  - (b) un'autorità TEMPEST (TA);
  - (c) un'autorità di approvazione degli apparati crittografici (CAA);
  - (d) un'autorità di distribuzione degli apparati crittografici (CDA).
9. A norma dell'articolo 7, paragrafo 7, della presente decisione, per ciascun sistema è stabilita:
  - (a) un'autorità di accreditamento di sicurezza (SAA);
  - (b) un'autorità operativa IA.
10. Le disposizioni di attuazione del presente articolo figurano nell'allegato A IV.

#### Articolo 9

#### **Sicurezza industriale**

1. Per "sicurezza industriale" si intende l'applicazione di misure che assicurino la protezione delle ICUE da parte di contraenti o subcontraenti in sede di negoziati precontrattuali e lungo tutto il ciclo di vita dei contratti classificati. Di norma, tali contratti non contemplano l'accesso alle informazioni classificate TRÈS SECRET UE/EU TOP SECRET.
2. Il SEAE può affidare per contratto mansioni che comportano o implicano l'accesso a, il trattamento o la conservazione di ICUE da parte di soggetti industriali o di altra natura registrati in uno Stato membro o in uno Stato terzo con cui sia stato concluso un accordo sulla sicurezza delle informazioni o un'intesa amministrativa conformemente all'articolo 10, paragrafo 1, dell'allegato A.
3. In quanto autorità contraente, il SEAE, nell'aggiudicare un contratto classificato a un soggetto industriale o di altra natura, assicura il rispetto delle norme minime sulla sicurezza industriale previste nella presente decisione e a cui fa riferimento il contratto. Esso assicura l'osservanza di tali norme minime attraverso la competente autorità di sicurezza nazionale (NSA)/autorità di sicurezza designata (DSA).
4. I contraenti o subcontraenti registrati in uno Stato membro partecipanti in contratti o subcontratti classificati che richiedono la gestione e conservazione di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nelle loro strutture, nell'esecuzione di tali contratti o nella fase precontrattuale, dispongono di un nulla osta di sicurezza delle imprese (FSC) del livello di classifica adatto, rilasciato dall'NSA, dalla DSA o da altra autorità di sicurezza competente di detto Stato membro.

5. Il personale del contraente o subcontraente che, per l'esecuzione di un contratto classificato, necessita dell'accesso ad informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET è in possesso di un nulla osta di sicurezza personale (PSC) rilasciato dalla rispettiva NSA, DSA o da altra autorità di sicurezza competente secondo le disposizioni legislative e regolamentari nazionali e le norme minime figuranti nell'allegato A I.
6. Le disposizioni di attuazione del presente articolo figurano nell'allegato A V.

#### Articolo 10

##### **Scambio di informazioni classificate con Stati terzi ed organizzazioni internazionali**

1. Il SEAE può scambiare ICUE con uno Stato terzo o un'organizzazione internazionale qualora:
  - (a) tra l'UE e tale Stato terzo o organizzazione internazionale sia in vigore un accordo sulla sicurezza delle informazioni concluso a norma dell'articolo 37 del TUE e dell'articolo 218 del TFUE; oppure
  - (b) tra l'AR e le competenti autorità di sicurezza di tale Stato terzo o organizzazione internazionale abbia acquisito efficacia un'intesa amministrativa per lo scambio di informazioni classificate, in linea di principio, di livello non superiore a RESTREINT UE/EU RESTRICTED, conclusa secondo la procedura di cui all'articolo 14, paragrafo 5, della presente decisione; oppure
  - (c) tra l'Unione europea e tale Stato terzo trovi applicazione un accordo quadro o ad hoc di partecipazione nell'ambito di una operazione PSDC di gestione delle crisi, concluso a norma dell'articolo 37 del TUE e dell'articolo 218 del TFUE,

e le condizioni stabilite in detto strumento siano state soddisfatte.

Le eccezioni alla regola generale di cui sopra sono riportate nell'allegato A VI, sezione V.

2. Le intese amministrative di cui al paragrafo 1, lettera b), contengono disposizioni intese ad assicurare che gli Stati terzi o le organizzazioni internazionali che ricevono le ICUE conferiscano loro una protezione appropriata al loro livello di classifica e conforme a norme minime non meno rigorose di quelle previste nella presente decisione.

Le informazioni scambiate sulla base degli accordi di cui al paragrafo 1, lettera c), sono limitate alle informazioni concernenti operazioni PSDC a cui lo Stato terzo in questione partecipa sulla base di tali accordi e in conformità delle rispettive disposizioni.

3. Per accertare l'efficacia delle misure di sicurezza poste in essere a protezione delle ICUE scambiate sono organizzate visite di valutazione negli Stati terzi o organizzazioni internazionali, come indicato all'articolo 16 della presente decisione.
4. La decisione di comunicare ad uno Stato terzo o ad una organizzazione internazionale ICUE detenute dal SEAE è presa caso per caso, in funzione della natura e del contenuto delle informazioni stesse, della necessità di conoscere del destinatario e dell'entità dei vantaggi per l'UE.

Il SEAE chiede il consenso scritto di ogni entità che abbia fornito informazioni classificate come materiale di base di ICUE originate dal SEAE stesso al fine di stabilire l'assenza di obiezioni al rilascio.

Se l'originatore delle informazioni classificate che si desiderano comunicare non è il SEAE, quest'ultimo chiede anzitutto il consenso scritto dell'originatore.

Tuttavia, se il SEAE non è in grado di stabilire l'originatore, l'autorità di sicurezza del SEAE si assume la responsabilità dell'originatore, previo parere favorevole unanime degli Stati membri rappresentati in seno al Comitato per la sicurezza del SEAE.

5. Le disposizioni di attuazione del presente articolo figurano nell'allegato A VI.

#### Articolo 11

##### **Violazione della sicurezza e compromissione di informazioni classificate**

1. Qualsiasi violazione o sospetta violazione della sicurezza e qualsiasi compromissione o sospetta compromissione di informazioni classificate è immediatamente riferita alla direzione "Sicurezza" del SEAE, che ne dà comunicazione, secondo il caso, alla direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione e al servizio di sicurezza del Segretariato generale del Consiglio, allo Stato membro o agli Stati membri interessati, o ad altri soggetti interessati.

2. Qualora sia noto o vi siano ragionevoli motivi per sospettare una compromissione o perdita di informazioni classificate, la direzione "Sicurezza" del SEAE informa la direzione "Sicurezza" della Commissione, il servizio di sicurezza del Segretariato generale del Consiglio o l'NSA dello Stato membro o degli Stati membri interessati, o gli altri soggetti interessati, secondo il caso, e adotta tutte le misure adeguate secondo le pertinenti disposizioni legislative e regolamentari al fine di:

- (a) valutare i potenziali danni agli interessi dell'UE o degli Stati membri;
- (b) adottare i provvedimenti opportuni per impedire che i fatti si ripetano;
- (c) conservare le prove;
- (d) assicurare che personale non direttamente interessato alla violazione indaghi sul caso per accertare i fatti;
- (e) informare le autorità competenti delle conseguenze dell'evento e delle misure adottate; nonché
- (f) informare l'originatore.

3. Ogni membro del personale sotto la responsabilità del SEAE che si renda responsabile di una violazione delle norme di sicurezza contenute nella presente decisione è passibile di un'azione disciplinare secondo le disposizioni normative e regolamentari applicabili.

Ogni persona responsabile della compromissione o della perdita di informazioni classificate è passibile di sanzioni disciplinari e/o azioni legali secondo le disposizioni legislative, normative e regolamentari applicabili.

La direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione, il servizio di sicurezza del Segretariato generale del Consiglio o l'NSA dello Stato membro o degli Stati membri interessati, o altri soggetti interessati ne sono immediatamente informati, secondo il caso.

4. Il Capo della direzione "Sicurezza" del SEAE può sospendere l'accesso della persona alle ICUE e ai locali del SEAE per tutta la durata delle indagini sulla violazione e/o compromissione. Di questa decisione sono immediatamente informati la direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione, il servizio di sicurezza del Segretariato generale del Consiglio o l'NSA dello Stato membro o degli Stati membri interessati, o gli altri soggetti interessati.

---

## ALLEGATO A I

## SICUREZZA PERSONALE

## I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 5 dell'allegato A. Stabilisce, in particolare, criteri che il SEAE applica per determinare se una persona, in considerazione della sua lealtà, onestà e affidabilità, può essere autorizzata ad accedere alle ICUE, nonché le procedure di indagine e amministrative da seguire a tal fine.
2. Il "nulla osta di sicurezza personale" (PSC) per l'accesso alle ICUE è una dichiarazione rilasciata da un'autorità competente di uno Stato membro al termine di un'indagine di sicurezza condotta dalle autorità competenti di uno Stato membro e attestante che una persona può avere accesso alle ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), e a una data stabilita, a condizione che sia stata accertata la sua necessità di conoscere; la persona così descritta è in possesso del "nulla osta di sicurezza".
3. Il "certificato di nulla osta di sicurezza personale" (PSCC) è un certificato rilasciato dall'autorità di sicurezza del SEAE che stabilisce che una persona è in possesso del nulla osta di sicurezza personale e in cui figura il livello di ICUE cui può accedere la persona in questione, la data di validità del relativo PSC nazionale e la data di scadenza del certificato stesso.
4. La "autorizzazione di accesso a ICUE" è un'autorizzazione rilasciata dall'autorità di sicurezza del SEAE ai sensi della presente decisione e previo rilascio di un PSC da parte delle competenti autorità di uno Stato membro, attestante che una persona può avere accesso a ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), e a una data stabilita, a condizione che sia stata accertata la sua necessità di conoscere. La persona così descritta è in possesso del "nulla osta di sicurezza personale".

## II. AUTORIZZAZIONE DI ACCESSO ALLE ICUE

5. L'accesso a informazioni classificate RESTREINT UE/EU RESTRICTED non richiede un nulla osta di sicurezza personale ed è rilasciato dopo che:
  - (a) sia stato stabilito un rapporto per legge o contratto tra la persona e il SEAE,
  - (b) sia stata accertata la necessità di conoscere della persona,
  - (c) la stessa sia stata istruita sulle norme e le procedure di sicurezza per la protezione delle ICUE ed abbia riconosciuto per iscritto la propria responsabilità in materia di protezione di tali informazioni conformemente alla presente decisione.
6. Una persona è autorizzata ad accedere ad informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore solo dopo che:
  - (a) sia stata accertata la sua necessità di conoscere;
  - (b) le sia stato concesso un PSC del livello adatto o sia in altro modo debitamente autorizzata in virtù delle sue funzioni conformemente alle disposizioni legislative e regolamentari nazionali; nonché
  - (c) sia stata istruita sulle norme e le procedure di sicurezza per la protezione delle ICUE ed abbia riconosciuto per iscritto la propria responsabilità in materia di protezione di tali informazioni.
7. Il SEAE individua all'interno delle sue strutture i posti che richiedono l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore e che richiedono pertanto un PSC del livello adatto, come indicato all'articolo 4.
8. Il personale del SEAE dichiara l'eventuale possesso della cittadinanza di più di un paese.

**Procedure di richiesta del PSC presso il SEAE**

9. Per il personale del SEAE, l'autorità di nomina del SEAE trasmette il questionario sulla sicurezza del personale compilato all'NSA dello Stato membro di cui è cittadino la persona interessata, chiedendo di avviare un'indagine di sicurezza per il livello di ICUE a cui la persona può chiedere di accedere.
10. Qualora una persona abbia la cittadinanza di più di un paese, la richiesta di indagini viene indirizzata all'NSA del paese con la cui nazionalità l'interessato è stato assunto.
11. Se viene a conoscenza di informazioni rilevanti per l'indagine di sicurezza relativa a una persona che ha chiesto un PSC, il SEAE le comunica all'NSA competente in conformità delle pertinenti disposizioni legislative e regolamentari.

12. Al termine dell'indagine di sicurezza l'NSA competente ne comunica l'esito alla direzione "Sicurezza" del SEAE.
- (a) Qualora dall'indagine di sicurezza emerga la garanzia dell'inesistenza di informazioni negative note che metterebbero in discussione la lealtà, l'onestà e l'affidabilità della persona, l'autorità di sicurezza del SEAE può rilasciare alla persona interessata un'autorizzazione di accesso a ICUE fino al livello adatto e a una data determinata.
- (b) Il SEAE adotta ogni opportuna misura per garantire che le condizioni e/o restrizioni imposte dall'NSA siano debitamente attuate. L'NSA sarà informata dell'esito.
- (c) Qualora dall'indagine di sicurezza non emerga tale garanzia, l'autorità di sicurezza del SEAE ne informa la persona interessata la quale può chiedere di essere ascoltata dall'autorità di sicurezza del SEAE. Quest'ultima può chiedere all'NSA competente ulteriori chiarimenti che è in grado di fornire conformemente alle sue disposizioni legislative e regolamentari nazionali. In caso di riconferma dell'esito, l'autorizzazione ad accedere alle ICUE non può essere concessa. In tal caso, il SEAE adotta misure idonee ad assicurare che al richiedente sia negato l'accesso alle ICUE.
13. L'indagine di sicurezza e i relativi risultati, su cui il SEAE fonda la decisione di concedere o meno un'autorizzazione ad accedere alle ICUE, sono soggetti alle pertinenti disposizioni legislative e regolamentari vigenti nello Stato membro in questione, ivi comprese quelle relative ai ricorsi. Le decisioni dell'autorità di sicurezza del SEAE sono soggette a ricorso conformemente allo statuto dei funzionari dell'Unione europea e al regime applicabile agli altri agenti dell'Unione europea, previsti nel regolamento (CEE, Euratom, CECA) n. 259/68 <sup>(1)</sup> (in seguito, "lo statuto").
14. La garanzia su cui è basato un PSC in corso di validità copre qualsiasi incarico della persona interessata all'interno del SEAE, del Segretariato generale del Consiglio o della Commissione.
15. Se il periodo di servizio di una persona non inizia entro dodici mesi dalla comunicazione dell'esito dell'indagine di sicurezza all'autorità di sicurezza del SEAE o se vi è un'interruzione del servizio di dodici mesi durante la quale la persona non ha occupato un posto presso il SEAE, in altre istituzioni, agenzie o organi UE, o nell'amministrazione di uno Stato membro, che richieda l'accesso a informazioni classificate, tale esito è sottoposto all'NSA competente affinché questa confermi se resta valido e pertinente.
16. Se viene a conoscenza di informazioni concernenti un rischio per la sicurezza posto da una persona in possesso di un PSC valido, il SEAE le comunica all'NSA competente in conformità alle pertinenti disposizioni legislative e regolamentari. Se un'NSA comunica al SEAE il ritiro della garanzia fornita in conformità al punto 12, lettera a) per una persona in possesso di un'autorizzazione valida per accedere a ICUE, l'autorità di sicurezza del SEAE può chiederle i chiarimenti che è in grado di fornire conformemente alle sue disposizioni legislative e regolamentari nazionali. Se le informazioni negative sono confermate, l'autorizzazione suddetta è ritirata e la persona in questione è esclusa dall'accesso alle ICUE e da posti nei quali tale accesso sia possibile o nei quali la persona potrebbe mettere a repentaglio la sicurezza.
17. La decisione di ritiro di un'autorizzazione di accesso alle ICUE a un membro del personale del SEAE e, se opportuno, i relativi motivi sono comunicati alla persona interessata la quale può chiedere di essere ascoltata dall'autorità di sicurezza del SEAE. Le informazioni fornite dall'NSA sono soggette alle pertinenti disposizioni legislative e regolamentari vigenti nello Stato membro in questione, ivi comprese quelle relative ai ricorsi. Le decisioni adottate dall'autorità di sicurezza del SEAE sono soggette a ricorso conformemente allo statuto.
18. Gli esperti nazionali distaccati presso il SEAE per un posto che richiede l'accesso alle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, presentano all'autorità di sicurezza del SEAE un valido PSC per l'accesso a ICUE di livello corrispondente prima di assumere l'incarico. Il processo summenzionato è gestito dallo Stato membro che procede al distacco.

#### **Registrazioni dei PSC**

19. Il SEAE mantiene una banca dati dello status dei nulla osta di sicurezza di tutto il personale posto sotto la sua responsabilità e del personale dei suoi contraenti. Questi dati comprendono il livello di ICUE cui può accedere la persona in questione (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), la data di concessione del PSC e il suo periodo di validità.
20. Procedure di coordinamento appropriate sono messe in atto con gli Stati membri e altre istituzioni, agenzie e organi dell'UE per garantire che il SEAE detenga dati completi sullo status dei nulla osta di sicurezza di tutto il personale posto sotto la sua responsabilità e del personale dei suoi contraenti.

<sup>(1)</sup> GU L 56 del 4.3.1968, pag. 1.

21. L'autorità di sicurezza del SEAE può rilasciare un certificato di nulla osta di sicurezza personale (PSCC) in cui figura il livello di ICUE cui può accedere la persona in questione (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), la data di validità del relativo PSC e la data di scadenza del certificato stesso.

#### **Esenzioni dall'obbligo del PSC**

22. Le persone debitamente autorizzate ad accedere alle ICUE in virtù delle rispettive funzioni, conformemente alle disposizioni legislative e regolamentari nazionali, sono informate, ove opportuno, dalla direzione "Sicurezza" del SEAE degli obblighi di sicurezza cui sono tenute per proteggere le ICUE.

### **III. FORMAZIONE E SENSIBILIZZAZIONE ALLA SICUREZZA**

23. Prima di essere autorizzate ad accedere a ICUE, tutte le persone attestano per iscritto di aver compreso gli obblighi di protezione delle ICUE e le conseguenze che possono verificarsi se le ICUE risultano compromesse. Una registrazione di tale attestazione scritta è conservata dal SEAE.

24. Tutte le persone che sono autorizzate ad avere accesso a ICUE o che le devono trattare, sono sensibilizzate all'inizio e istruite periodicamente riguardo alle minacce per la sicurezza e devono comunicare immediatamente alle autorità di sicurezza competenti qualsiasi approccio o attività che ritengano sospetto o inusuale.

25. Tutte le persone cui è consentito l'accesso alle ICUE devono essere sottoposte a costanti misure di sicurezza del personale (ossia accompagnamento costante) per tutto il tempo in cui trattano ICUE. Della sicurezza del personale sono responsabili:

(a) le persone cui è stato consentito l'accesso alle ICUE: sono responsabili personalmente della propria condotta sotto il profilo della sicurezza e devono comunicare immediatamente alle competenti autorità di sicurezza qualsiasi approccio o attività a loro giudizio sospetti o inusuali e i cambiamenti eventualmente intervenuti nella loro situazione personale che possano incidere sul loro PSC o sull'autorizzazione ad accedere a ICUE;

(b) i superiori gerarchici: sono tenuti a garantire che il personale sia a conoscenza delle misure di sicurezza e delle responsabilità in materia di protezione delle ICUE, a vigilare sulla condotta del personale sotto il profilo della sicurezza e ad occuparsi direttamente di eventuali questioni di sicurezza o a comunicare alle autorità di sicurezza competenti ogni informazione negativa che possa incidere sul PSC o sull'autorizzazione del personale ad accedere alle ICUE;

(c) gli operatori dell'organizzazione della sicurezza del SEAE di cui all'articolo 12 della presente decisione: hanno il compito di sensibilizzare sulla sicurezza il personale del proprio settore attraverso sessioni informative periodiche, di promuovere una solida cultura della sicurezza nel settore di loro competenza, di attuare misure volte a vigilare sulla condotta del personale sotto il profilo della sicurezza e di comunicare alle autorità di sicurezza competenti tutte le informazioni negative che possano incidere sul PSC di qualsiasi persona;

(d) il SEAE e gli Stati membri: predispongono i canali necessari a comunicare le informazioni che possano incidere sul PSC o sull'autorizzazione di qualsiasi persona ad accedere alle ICUE.

26. Tutte le persone che cessano l'incarico per il quale era richiesto l'accesso alle ICUE sono informate sull'obbligo di continuare a proteggere le ICUE e, in caso, riconoscono per iscritto quest'obbligo.

### **IV. CIRCOSTANZE ECCEZIONALI**

27. Per motivi di urgenza, se debitamente giustificati nell'interesse del SEAE e in attesa che sia ultimata l'indagine di sicurezza nel suo insieme, l'autorità di sicurezza del SEAE, dopo aver consultato l'NSA dello Stato membro di cui è cittadino la persona interessata e con riserva dell'esito dei controlli preliminari per verificare l'inesistenza di informazioni negative note, può rilasciare un'autorizzazione temporanea ai funzionari e altri agenti del SEAE per accedere alle ICUE per una funzione specifica. L'indagine di sicurezza deve essere completata il più rapidamente possibile. Tali autorizzazioni temporanee sono valide per sei mesi al massimo e non danno accesso alle informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET. Tutte le persone alle quali è stata concessa un'autorizzazione temporanea attestano per iscritto di aver compreso gli obblighi di protezione delle ICUE e le conseguenze che possono verificarsi se le ICUE risultano compromesse. Una registrazione di tale attestazione scritta è conservata dal SEAE.

28. Quando a una persona deve essere assegnato un posto che richiede un PSC di un livello superiore a quello posseduto in quel momento dalla persona stessa, l'incarico può essere affidato in via provvisoria purché:

(a) il superiore gerarchico della persona in questione giustifichi per iscritto che l'accesso a ICUE di livello superiore è assolutamente necessario;

(b) l'accesso sia limitato a specifici elementi delle ICUE in relazione con l'incarico;

- (c) la persona sia in possesso di un PSC valido;
  - (d) si sia dato avvio alla procedura per ottenere l'autorizzazione per il livello di accesso richiesto per il posto in questione;
  - (e) siano stati effettuati controlli soddisfacenti dall'autorità competente, volti ad accertare che la persona non ha violato seriamente o ripetutamente le norme di sicurezza;
  - (f) l'incarico della persona sia approvato dalla competente autorità del SEAE; nonché
  - (g) l'NSA/DSA competente che ha rilasciato il PSC della persona in questione sia stata consultata e non abbia formulato obiezioni;
  - (h) la deroga sia conservata nell'ufficio di registrazione responsabile o suo ufficio dipendente con una descrizione delle informazioni per cui è stato approvato l'accesso.
29. La procedura sopra descritta si usa per l'accesso singolo a ICUE di un livello superiore a quello autorizzato dal nulla osta della persona in questione. Tale procedura non è usata in maniera ricorrente.
30. In circostanze del tutto eccezionali, quali missioni in ambienti ostili o in periodi di tensione internazionale crescente quando richiesto da misure di emergenza, soprattutto per salvare vite umane, l'Alto rappresentante, il Segretario generale esecutivo o il direttore esecutivo possono concedere, se possibile per iscritto, l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET a persone che non posseggono il PSC richiesto, purché ciò sia assolutamente necessario e non vi siano dubbi ragionevoli sulla lealtà, onestà e affidabilità delle persone in questione. La registrazione di tale autorizzazione è conservata con una descrizione delle informazioni per cui è stata data.
31. Nel caso di informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET, questo accesso di emergenza è limitato a cittadini UE autorizzati ad accedere a informazioni il cui livello di classifica nazionale equivale a TRÈS SECRET UE/EU TOP SECRET o a informazioni classificate di livello SECRET UE/EU SECRET.
32. Il Comitato per la sicurezza del SEAE è informato dei casi in cui si ricorre alla procedura descritta ai punti 29 e 30.
33. Il Comitato per la sicurezza del SEAE riceve una relazione annuale sul ricorso alle procedure stabilite nella presente sezione.

#### V. PARTECIPAZIONE A RIUNIONI NELLA SEDE CENTRALE DEL SEAE E NELLE DELEGAZIONI DELL'UNIONE.

34. Le persone che devono partecipare a riunioni presso la sede centrale del SEAE e nelle delegazioni dell'Unione in cui sono discusse informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, possono farlo solo se confermato dallo status del PSC in loro possesso. Per i rappresentanti degli Stati membri, i funzionari del Segretariato generale del Consiglio e della Commissione, il PSCC o altra prova di PSC è trasmesso dalle autorità competenti alla direzione "Sicurezza" del SEAE, al coordinatore della sicurezza della delegazione dell'Unione o, in via eccezionale, è presentato dall'interessato stesso. Se del caso, può essere usato un elenco di nomi consolidato che compri il PSC.
35. Se il PSC per l'accesso alle ICUE è ritirato a una persona i cui compiti richiedono la partecipazione a riunioni presso la sede centrale del SEAE o nelle delegazioni dell'Unione nelle quali si discutono informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, l'autorità competente ne informa il SEAE.

#### VI. ACCESSO POTENZIALE ALLE ICUE

36. Le persone che devono essere impiegate in circostanze nelle quali potrebbero avere un potenziale accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, ottengono il nulla osta di sicurezza adatto o sono scortate in ogni momento.
37. Corrieri, guardie e scorte ottengono il nulla osta di sicurezza di livello adatto o sono soggetti alle opportune indagini in conformità alle disposizioni legislative e regolamentari nazionali e sono informati periodicamente riguardo alle procedure di sicurezza in materia di protezione delle ICUE e sugli obblighi di protezione delle informazioni di tale natura loro affidate o alle quali possono involontariamente avere accesso.

## ALLEGATO A II

**SICUREZZA MATERIALE DELLE INFORMAZIONI CLASSIFICATE UE****I. INTRODUZIONE**

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 6 dell'allegato A. Esso stabilisce requisiti minimi per la protezione materiale di locali, edifici, uffici, stanze e altre zone in cui sono trattate e conservate ICUE, nonché le zone in cui sono conservati i CIS.
2. Le misure di sicurezza materiale sono intese ad evitare l'accesso non autorizzato alle ICUE:
  - (a) assicurando che le ICUE siano trattate e conservate in modo adeguato;
  - (b) consentendo la differenziazione del personale per quanto riguarda l'accesso alle ICUE in base alla necessità di conoscere e, in caso, ai rispettivi nulla osta di sicurezza;
  - (c) scoraggiando, ostacolando e scoprendo azioni non autorizzate; nonché
  - (d) impedendo o ritardando l'ingresso fraudolento o con la forza di intrusi.

**II. REQUISITI E MISURE DI SICUREZZA MATERIALE**

3. Il SEAE applica una procedura di gestione del rischio per proteggere le ICUE nei propri locali al fine di garantire un livello di protezione materiale corrispondente alla valutazione del rischio. La procedura di gestione del rischio tiene conto di tutti gli elementi pertinenti, in particolare:
  - (a) del livello di classifica delle ICUE;
  - (b) della forma e del volume delle ICUE, tenendo conto che considerevoli quantitativi o compilazioni di ICUE possono richiedere l'applicazione di misure di protezione più rigorose;
  - (c) dell'ambiente circostante e della struttura degli edifici o delle zone in cui sono conservate ICUE;
  - (d) della valutazione della minaccia del paese terzo effettuata dall'INTCEN, in particolare sulla base delle relazioni della delegazione dell'Unione, e
  - (e) della valutazione della minaccia rappresentata da servizi di intelligence che prendono di mira l'UE o gli Stati membri e da atti di sabotaggio, terrorismo e altri atti sovversivi o criminali.
4. Nell'applicare il concetto di difesa in profondità, l'autorità di sicurezza del SEAE stabilisce l'idonea combinazione di misure di sicurezza materiale da attuare. Queste ultime possono comprendere una o più delle seguenti misure:
  - (a) barriera perimetrale: barriera materiale che difende i confini della zona richiedente protezione;
  - (b) sistemi di rilevamento delle intrusioni (IDS): un IDS può essere usato per accrescere il livello di sicurezza fornito dalla barriera perimetrale, oppure in stanze ed edifici al posto del personale addetto alla sicurezza o in ausilio a quest'ultimo;
  - (c) controllo dell'accesso: il controllo dell'accesso può essere esercitato su un sito, un edificio o più edifici in un sito, o su zone o stanze all'interno di un edificio. Il controllo può essere effettuato mediante dispositivi elettronici o elettromeccanici, dal personale addetto alla sicurezza e/o da un addetto all'accoglienza, o con altri mezzi materiali;
  - (d) personale addetto alla sicurezza: formato e controllato e, ove necessario, munito di apposito nulla osta di sicurezza, può essere impiegato, tra l'altro, come deterrente contro individui che progettano un'intrusione dissimulata;
  - (e) televisione a circuito chiuso (CCTV): la CCTV può essere usata dal personale addetto alla sicurezza per verificare incidenti e allarmi provenienti da IDS in siti o perimetri estesi;
  - (f) illuminazione di sicurezza: l'illuminazione di sicurezza può essere usata come deterrente contro intrusioni potenziali nonché per fornire l'illuminazione necessaria per una sorveglianza efficace diretta da parte del personale addetto alla sicurezza o indiretta attraverso un sistema di CCTV; nonché

(g) eventuali altre misure materiali volte a scoraggiare o scoprire l'accesso non autorizzato o a evitare la perdita o il danneggiamento di ICUE.

5. La direzione "Sicurezza" del SEAE può effettuare ispezioni all'entrata e all'uscita come deterrente all'introduzione non autorizzata di materiale o alla sottrazione non autorizzata di ICUE da locali o edifici.
6. Quando le ICUE sono a rischio di sguardi indiscreti, anche accidentalmente, sono adottate misure appropriate per combattere questo rischio.
7. Per le nuove strutture sono definiti requisiti di sicurezza materiale e relative specifiche funzionali nell'ambito della pianificazione e della concezione delle strutture stesse. Per le strutture esistenti si applicano il più possibile i requisiti di sicurezza materiale.

### III. ATTREZZATURE PER LA PROTEZIONE MATERIALE DELLE ICUE

8. Nell'acquistare attrezzature (quali contenitori di sicurezza, macchine sminuzzatrici, serrature di porte, sistemi elettronici di controllo dell'accesso, IDS, sistemi d'allarme) per la protezione materiale delle ICUE, l'autorità di sicurezza del SEAE garantisce che tali attrezzature siano conformi alle norme tecniche e ai requisiti minimi approvati.
9. Le specifiche tecniche delle attrezzature da utilizzare per la protezione materiale delle ICUE figurano negli orientamenti di sicurezza che devono essere approvati dal Comitato per la sicurezza del SEAE.
10. I sistemi di sicurezza sono ispezionati a intervalli regolari e le attrezzature sono regolarmente sottoposte a manutenzione. I lavori di manutenzione tengono conto del risultato delle ispezioni per garantire il costante funzionamento ottimale delle attrezzature.
11. L'efficacia delle singole misure di sicurezza nonché del sistema di sicurezza nel suo complesso è oggetto di una nuova valutazione ad ogni ispezione.

### IV. ZONE OGGETTO DI PROTEZIONE MATERIALE

12. Per la protezione materiale delle ICUE si stabiliscono due tipi di zona oggetto di protezione materiale o relativi equivalenti nazionali:
  - (a) zone amministrative e
  - (b) zone protette (comprese le zone protette tecnicamente).
13. L'autorità di sicurezza del SEAE stabilisce che una zona soddisfa i requisiti per essere designata zona amministrativa, zona protetta o zona protetta tecnicamente.
14. Per le zone amministrative:
  - (a) è stabilito un perimetro chiaramente delimitato che permette l'ispezione delle persone e, se possibile, dei veicoli;
  - (b) l'accesso senza scorta è consentito solo alle persone debitamente autorizzate dalla direzione "Sicurezza" del SEAE; nonché
  - (c) tutte le altre persone sono scortate in ogni momento o sottoposte a controlli equivalenti.
15. Per le zone protette:
  - (a) è stabilito un perimetro chiaramente delimitato e protetto attraverso cui sono controllati tutti gli ingressi e le uscite per mezzo di un lasciapassare o di un sistema di riconoscimento personale;
  - (b) l'accesso senza scorta è consentito solo alle persone in possesso di un nulla osta di sicurezza del livello adatto ed espressamente autorizzate ad entrare nella zona in base alla loro necessità di conoscere;
  - (c) tutte le altre persone sono scortate in ogni momento o sottoposte a controlli equivalenti.
16. Se l'ingresso in una zona protetta costituisce, a tutti i fini pratici, un accesso diretto alle informazioni classificate ivi conservate, si applicano i seguenti requisiti supplementari:
  - (a) il livello più elevato di classifica di sicurezza delle informazioni normalmente conservate nella zona è chiaramente indicato;

- (b) tutti i visitatori richiedono un'autorizzazione specifica ad entrare nella zona, sono scortati in ogni momento e sono in possesso del nulla osta di sicurezza adatto, a meno che non siano presi provvedimenti intesi a garantire che non sia possibile alcun accesso alle ICUE;
  - (c) i dispositivi elettronici sono lasciati fuori della zona.
17. Le zone protette che vengono messe al riparo dall'ascolto indiscreto sono designate zone protette tecnicamente. Si applicano i seguenti requisiti supplementari:
- (a) tali zone sono dotate di IDS, chiuse a chiave se non occupate e sorvegliate se occupate. Tutte le chiavi sono controllate in conformità della sezione VI dell'allegato;
  - (b) tutte le persone e tutto il materiale che accedono a tali zone sono soggetti a controllo;
  - (c) tali zone sono regolarmente soggette a ispezioni materiali e/o tecniche, come richiesto dall'autorità di sicurezza del SEAE. Dette ispezioni sono inoltre effettuate dopo qualsiasi ingresso non autorizzato, effettivo o sospettato; nonché
  - (d) tali zone sono prive di linee di comunicazione non autorizzate, telefoni o altri dispositivi di comunicazione ed attrezzature elettriche o elettroniche non autorizzati.
18. Nonostante il punto 17, lettera d), prima di essere usati in zone in cui si svolgono riunioni o attività che implicano informazioni classificate di livello SECRET UE/EU SECRET o superiore, e laddove la minaccia alle ICUE sia valutata alta, tutti i dispositivi di comunicazione e tutte le attrezzature elettriche o elettroniche sono preventivamente esaminati dall'autorità di sicurezza del SEAE al fine di garantire che nessuna informazione intelligibile sia trasmessa inavvertitamente o illegalmente da tali attrezzature all'esterno del perimetro della zona protetta.
19. Ove opportuno, le zone protette non occupate da personale in servizio 24 ore su 24 sono ispezionate al termine del normale orario di lavoro e a intervalli casuali al di fuori del normale orario di lavoro, tranne nel caso in cui vi sia installato un IDS.
20. Le zone protette e le zone protette tecnicamente possono essere istituite in via temporanea in una zona amministrativa per una riunione classificata o per altri motivi analoghi.
21. Per ciascuna zona protetta sono elaborate procedure operative di sicurezza che stabiliscono:
- (a) il livello delle ICUE che possono essere trattate e conservate nella zona;
  - (b) le misure di sorveglianza e di protezione che devono essere applicate;
  - (c) le persone autorizzate ad accedere senza scorta alla zona in virtù della loro necessità di conoscere e del loro nulla osta di sicurezza;
  - (d) ove opportuno, le procedure relative alle scorte o alla protezione delle ICUE quando si autorizza l'accesso di altre persona alla zona;
  - (e) ogni altra misura e procedura pertinente.
22. Nelle zone protette sono costruite camere blindate. Le pareti, il pavimento, il soffitto, le finestre e le porte provviste di serratura sono approvati dall'autorità di sicurezza del SEAE e offrono una protezione equivalente a quella di un contenitore di sicurezza approvato per la conservazione di ICUE dello stesso livello di classifica.
- V. MISURE DI PROTEZIONE MATERIALE PER IL TRATTAMENTO E LA CONSERVAZIONE DELLE ICUE**
23. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED possono essere trattate:
- (a) in una zona protetta;
  - (b) in una zona amministrativa purché le ICUE siano protette dall'accesso di persone non autorizzate; o
  - (c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore trasporti le ICUE in conformità dell'allegato A III, punti da 30 a 42, e si sia impegnato ad osservare le misure compensative stabilite nelle istruzioni di sicurezza emesse dall'autorità di sicurezza del SEAE per garantire che le ICUE siano protette dall'accesso di persone non autorizzate.

24. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED sono conservate in idonei mobili da ufficio chiusi a chiave, in una zona amministrativa o in una zona protetta. Esse possono essere temporaneamente conservate all'esterno di una zona protetta o di una zona amministrativa purché il detentore si sia impegnato ad osservare le misure compensative stabilite nelle istruzioni di sicurezza emesse dall'autorità di sicurezza del SEAE.
25. Le ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET possono essere trattate:
- (a) in una zona protetta;
  - (b) in una zona amministrativa purché le ICUE siano protette dall'accesso di persone non autorizzate; oppure
  - (c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore:
    - (i) trasporti le ICUE in conformità dell'allegato A III, punti da 30 a 42;
    - (ii) si sia impegnato ad osservare le misure compensative stabilite nelle istruzioni di sicurezza emesse dall'autorità di sicurezza del SEAE per garantire che le ICUE siano protette dall'accesso di persone non autorizzate;
    - (iii) tenga le ICUE sempre sotto il proprio controllo; nonché
    - (iv) in caso di documenti cartacei, ne abbia informato il competente ufficio di registrazione.
26. Le ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET sono conservate in una zona protetta, in un contenitore di sicurezza o in una camera blindata.
27. Le ICUE classificate di livello TRÈS SECRET UE/EU TOP SECRET sono trattate in una zona protetta.
28. Le ICUE classificate di livello TRÈS SECRET UE/EU TOP SECRET sono conservate in una zona protetta presso la sede centrale, secondo una delle modalità seguenti:
- (a) in un contenitore di sicurezza conformemente al punto 8, con uno o più dei seguenti controlli supplementari:
    - (i) protezione continua o verifica da parte di personale con nulla osta di sicurezza o personale di servizio;
    - (ii) un IDS approvato, in combinazione con personale di sicurezza incaricato degli interventi;oppure
  - (b) in una camera blindata dotata di IDS, in combinazione con personale di sicurezza incaricato degli interventi.
29. Le norme sul trasporto di ICUE al di fuori delle zone oggetto di protezione materiale figurano nell'allegato A III.
- VI. CONTROLLO DELLE CHIAVI E DELLE COMBINAZIONI USATE PER PROTEGGERE LE ICUE**
30. L'autorità di sicurezza del SEAE stabilisce le procedure di gestione delle chiavi e delle combinazioni per gli uffici, le stanze, le camere blindate e i contenitori di sicurezza. Tali procedure proteggono dall'accesso non autorizzato.
31. Le combinazioni sono conosciute a memoria dal minor numero possibile di persone che ha necessità di conoscerle. Le combinazioni dei contenitori di sicurezza e delle camere blindate in cui sono conservate ICUE sono modificate:
- (a) al ricevimento di ogni nuovo contenitore;
  - (b) in caso di sostituzione del personale che conosce la combinazione;
  - (c) in caso di effettiva o sospetta compromissione;
  - (d) se una serratura è stata oggetto di manutenzione o riparazione; nonché
  - (e) almeno ogni dodici mesi.
-

## ALLEGATO A III

**GESTIONE DELLE INFORMAZIONI CLASSIFICATE****I. INTRODUZIONE**

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 7 dell'allegato A. Esso stabilisce le misure amministrative per controllare le ICUE per tutto il loro ciclo di vita al fine di contribuire a scoraggiare, scoprire e porre rimedio ai casi di compromissione o perdita intenzionale o accidentale di tali informazioni.

**II. GESTIONE DELLE CLASSIFICHE****Classifiche e contrassegni**

2. Le informazioni sono classificate quando devono essere protette con riferimento alla loro riservatezza.
3. L'originatore delle ICUE è incaricato di determinare il livello di classifica di sicurezza, conformemente ai pertinenti orientamenti in materia di classifica, e della diffusione delle informazioni.
4. Il livello di classifica delle ICUE è stabilito conformemente all'articolo 2, paragrafo 2 dell'allegato A e con riferimento alla politica di sicurezza che deve essere approvata ai sensi dell'articolo 3, paragrafo 3, dell'allegato A.
5. Alle informazioni degli Stati membri scambiate con il SEAE sarà conferito lo stesso livello di protezione delle ICUE classificate ad un livello equivalente. Una tabella delle equivalenze è riportata nell'appendice B della decisione 2011/292/UE del Consiglio, del 31 marzo 2011, sulle norme di sicurezza per la protezione delle informazioni classificate UE.
6. La classifica di sicurezza e, se del caso, la data o un evento specifico a seguito dei quali possono essere declassate o declassificate, è chiaramente e correttamente indicata, indipendentemente dal fatto che le ICUE siano in forma cartacea, orale, elettronica o in altra forma.
7. Le singole parti di un determinato documento (ad esempio pagine, paragrafi, sezioni, annessi, appendici, allegati e materiale accluso) possono richiedere classifiche differenti e sono contraddistinte di conseguenza anche nel caso in cui siano conservate in forma elettronica.
8. Per quanto possibile, i documenti che contengono parti con livelli di classifica diversi sono impostati in modo che le parti con un livello di classifica diverso possano essere facilmente individuate e, se necessario, separate.
9. Il livello generale di classifica di un documento o file è almeno quello del suo componente con livello di classifica più elevato. Quando si riprendono informazioni da varie fonti, il prodotto finale è riesaminato per determinarne il livello generale di classifica di sicurezza, in quanto può richiedere una classifica più elevata di quella dei suoi componenti.
10. La classifica di una lettera o di una nota che comprende materiale accluso corrisponde a quello dell'elemento accluso con livello di classifica più elevato. L'originatore indica chiaramente il livello di classifica della lettera o della nota quando è separata dal materiale accluso mediante un contrassegno adeguato, ad esempio:

CONFIDENTIEL UE/EU CONFIDENTIAL

Senza allegato/i RESTREINT UE/EU RESTRICTED

**Contrasegni**

11. Oltre ad uno dei contrassegni di classifica di sicurezza di cui all'articolo 2, paragrafo 2, dell'allegato A, le ICUE possono recare altri contrassegni, quali:
  - (a) un identificatore per designare l'originatore;
  - (b) avvertenze, parole chiave o acronimi per specificare il settore di attività cui si riferisce il documento, una distribuzione particolare sulla base del principio della necessità di conoscere o restrizioni d'uso;
  - (c) contrassegni di divulgabilità.
12. A seguito di una decisione di comunicare ICUE a uno Stato terzo o ad un'organizzazione internazionale, la direzione "Sicurezza" del SEAE trasmette le informazioni classificate in questione con apposto un contrassegno di divulgabilità che indica lo Stato terzo o l'organizzazione internazionale a cui saranno comunicate.

13. Un elenco dei contrassegni autorizzati sarà adottato dall'autorità di sicurezza del SEAE.

#### **Contrassegni di classifica abbreviati**

14. Contrassegni di classifica abbreviati standard possono essere usati per indicare il livello di classifica di singoli paragrafi di un testo. Le abbreviazioni non sostituiscono i contrassegni di classifica per esteso.
15. Le seguenti abbreviazioni standard possono essere usate nei documenti classificati UE per indicare il livello di classifica di sezioni o parti del testo di dimensioni inferiori a una pagina:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

#### **Creazione di ICUE**

16. Quando si produce un documento classificato UE:
- (a) ciascuna pagina è contrassegnata chiaramente con il livello di classifica;
  - (b) ciascuna pagina è numerata;
  - (c) il documento reca un numero di riferimento e un oggetto che non è in sé un'informazione classificata, a meno che non sia contrassegnato come tale;
  - (d) il documento è datato;
  - (e) i documenti classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, se devono essere distribuiti in più copie, recano un numero di copia su ciascuna pagina.
17. Qualora non sia possibile applicare il punto 15 alle ICUE, sono adottate altre misure appropriate conformemente agli orientamenti di sicurezza che devono essere stabiliti a norma della presente decisione.

#### **Declassamento e declassificazione delle ICUE**

18. Al momento della creazione, l'originatore indica, laddove possibile e in particolare per le informazioni classificate RESTREINT UE/EU RESTRICTED, se le ICUE possono essere declassate o declassificate ad una certa data o in seguito ad un dato evento.
19. Il SEAE riesamina periodicamente le ICUE in suo possesso per accertare che il livello di classifica sia ancora applicabile. Il SEAE predispose un sistema per riesaminare il livello di classifica delle ICUE registrate che ha originato almeno ogni cinque anni. Tale riesame non è necessario se l'originatore ha indicato fin dall'inizio la data esatta in cui le informazioni saranno automaticamente declassate o declassificate e se le informazioni sono state contrassegnate di conseguenza.

### **III. REGISTRAZIONE DI ICUE A FINI DI SICUREZZA**

20. È istituito presso la sede centrale un ufficio centrale di registrazione. Per tutte le entità organizzative nel SEAE, nelle quali sono trattate ICUE, è istituito un ufficio di registrazione competente, subordinato all'ufficio centrale di registrazione, che provvede affinché le ICUE siano trattate conformemente alla presente decisione. Gli uffici di registrazione sono costituiti come zone protette definite nell'allegato A.

Ciascuna delegazione dell'Unione istituisce il proprio ufficio di registrazione delle ICUE.

Per questi uffici di registrazione l'autorità di sicurezza del SEAE designa un capo dell'ufficio di registrazione.

21. Ai fini della presente decisione, per registrazione a fini di sicurezza ("registrazione") si intende l'applicazione di procedure che registrano il ciclo di vita delle informazioni, ivi comprese la diffusione e la distruzione. Nel caso di un CIS, le procedure di registrazione possono essere eseguite mediante procedure interne allo stesso CIS.

22. Tutto il materiale classificato di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore è registrato quando entra o lascia un'entità organizzativa, comprese le delegazioni dell'Unione. Le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET sono registrate in uffici di registrazione dedicati.
23. L'ufficio centrale di registrazione costituisce, presso la sede centrale del SEAE, il principale punto di entrata ed uscita degli scambi di informazioni classificate con Stati terzi e organizzazioni internazionali. Esso conserva una registrazione di tutti tali scambi.
24. L'AR approva una politica di sicurezza sulla registrazione delle ICUE a fini di sicurezza, in conformità all'articolo 14 della presente decisione.

#### **Uffici di registrazione très secret UE/EU top secret**

25. Nella sede centrale del SEAE è designato un ufficio centrale di registrazione che funge da autorità centrale ricevente e trasmittente per le informazioni classificate TRÈS SECRET UE/EU TOP SECRET. Per il trattamento di tali informazioni a fini di registrazione possono essere designati, se necessario, uffici dipendenti.
26. Tali uffici dipendenti non possono trasmettere documenti di livello TRÈS SECRET UE/EU TOP SECRET direttamente ad altri uffici dipendenti dello stesso ufficio centrale di registrazione TRÈS SECRET UE/EU TOP SECRET o all'esterno senza l'approvazione esplicita di quest'ultimo.

#### **IV. RIPRODUZIONE E TRADUZIONE DI DOCUMENTI CLASSIFICATI UE**

27. I documenti di livello TRÈS SECRET UE/EU TOP SECRET possono essere riprodotti o tradotti solo previo consenso scritto dell'originatore.
28. Se l'originatore di documenti classificati di livello SECRET UE/EU SECRET o inferiore non ha imposto limitazioni alla riproduzione o alla traduzione, detti documenti possono essere riprodotti o tradotti su istruzione del detentore.
29. Le misure di sicurezza applicabili al documento originale si applicano alle copie e alle traduzioni. Le copie di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono create solo da un competente ufficio di registrazione o ufficio di registrazione dipendente per mezzo di una fotocopiatrice protetta. Le copie devono essere registrate.

#### **V. TRASPORTO DELLE ICUE**

30. Il trasporto di ICUE è soggetto alle misure di protezione menzionate nei punti da 31 a 41. Se le ICUE sono trasportate con mezzi elettronici, e in deroga all'articolo 7, paragrafo 4, dell'allegato A, le misure di protezione di seguito descritte possono essere integrate da opportune contromisure tecniche prescritte dall'autorità di sicurezza del SEAE per minimizzare il rischio di perdita o di compromissione.
31. L'autorità di sicurezza del SEAE impartisce istruzioni relative al trasporto di ICUE conformemente alla presente decisione.

#### **All'interno di un edificio o di un gruppo autonomo di edifici**

32. Le ICUE trasportate all'interno di un edificio o di un gruppo autonomo di edifici sono occultate per impedire che ne sia osservato il contenuto.
33. All'interno di un edificio o di un gruppo autonomo di edifici, le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET sono trasportate da persone in possesso del nulla osta di sicurezza di livello adatto in una busta protetta recante unicamente il nome del destinatario.

#### **All'interno dell'UE**

34. Le ICUE trasportate tra edifici o locali all'interno dell'UE sono racchiuse in plichi in modo da proteggerle da divulgazione non autorizzata.
35. Il trasporto di informazioni classificate fino al livello SECRET UE/EU SECRET all'interno dell'UE è effettuato secondo una delle seguenti modalità:
  - (a) corriere militare, governativo o valigia diplomatica, secondo i casi;
  - (b) trasporto a mano, a condizione che:
    - (i) le ICUE siano sempre detenute dal latore, a meno che non siano conservate conformemente ai requisiti di cui all'allegato A II;
    - (ii) le ICUE non siano aperte durante il trasporto, né lette in luoghi pubblici;

- (iii) le persone siano dotate del nulla osta di sicurezza del livello adatto e informate delle loro responsabilità in materia di sicurezza;
  - (iv) le persone dispongano, se necessario, di un certificato di corriere;
- (c) servizi postali o servizi di corriere commerciale, a condizione che:
- (i) siano approvati dall'NSA competente in conformità delle disposizioni legislative e regolamentari nazionali;
  - (ii) applichino adeguate misure di protezione in conformità dei requisiti minimi da stabilire negli orientamenti di sicurezza a norma dell'articolo 20, paragrafo 1 della presente decisione.

In caso di trasporto da uno Stato membro all'altro, le disposizioni della lettera c) sono limitate alle informazioni classificate fino al livello CONFIDENTIEL UE/EU CONFIDENTIAL.

36. Il materiale classificato CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET (ad esempio attrezzature o macchinari), che non può essere trasportato secondo le modalità di cui al punto 34, è trasportato come carico da società di vettori commerciali conformemente all'allegato A V.
37. Il trasporto di informazioni classificate TRÈS SECRET UE/EU TOP SECRET tra edifici o locali all'interno dell'UE è effettuato per corriere militare, governativo o valigia diplomatica, secondo i casi.

#### **Dall'UE al territorio di uno Stato terzo, o tra entità dell'UE in Stati terzi**

38. Le ICUE trasportate dall'UE al territorio di uno Stato terzo, o tra entità dell'UE in Stati terzi, sono racchiuse in plichi in modo da proteggerle da divulgazione non autorizzata.
39. Il trasporto di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET dall'UE al territorio di uno Stato terzo, e il trasporto di ICUE classificate fino al livello SECRET UE/EU SECRET tra entità dell'UE in Stati terzi, è effettuato secondo una delle seguenti modalità:
- (a) corriere militare o valigia diplomatica;
  - (b) trasporto a mano, a condizione che:
    - (i) il plico rechi un sigillo ufficiale o l'indicazione che è una consegna ufficiale non soggetta a controllo doganale o di sicurezza;
    - (ii) le persone dispongano di un certificato di corriere che identifica il plico e le autorizza a trasportarlo;
    - (iii) le ICUE siano sempre detenute dal latore, a meno che non siano conservate conformemente ai requisiti di cui all'allegato A II;
    - (iv) le ICUE non siano aperte durante il trasporto, né lette in luoghi pubblici; nonché
    - (v) le persone siano dotate del nulla osta di sicurezza del livello adatto e informate delle loro responsabilità in materia di sicurezza.
40. Il trasporto di informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET comunicate dall'UE a uno Stato terzo o ad un'organizzazione internazionale è conforme alle pertinenti disposizioni previste in un accordo sulla sicurezza delle informazioni o un'intesa amministrativa in conformità dell'articolo 10, paragrafo 2, dell'allegato A.
41. Le informazioni classificate RESTREINT UE/EU RESTRICTED possono essere trasportate dall'UE al territorio di uno Stato terzo anche con servizi postali o servizi di corriere commerciale.
42. Il trasporto di informazioni classificate TRÈS SECRET UE/EU TOP SECRET dall'UE al territorio di uno Stato terzo, o tra entità dell'UE in Stati terzi, è effettuato per corriere militare o valigia diplomatica.

#### **VI. DISTRUZIONE DI ICUE**

43. I documenti classificati UE che non sono più necessari possono essere distrutti, fatti salvi norme e regolamenti pertinenti in materia di archiviazione.

44. I documenti soggetti a registrazione ai sensi dell'articolo 7, paragrafo 2, dell'allegato A sono distrutti dall'ufficio di registrazione competente su istruzione del detentore o di un'autorità competente. I repertori e gli altri dati sulla registrazione sono aggiornati di conseguenza.
45. Per i documenti classificati SECRET UE/EU SECRET o TRÈS SECRET UE/EU TOP SECRET la distruzione avviene in presenza di un testimone che possiede un nulla osta di sicurezza almeno del livello di classifica del documento da distruggere.
46. L'ufficiale del registro e il testimone, laddove sia richiesta la presenza di quest'ultimo, firmano un certificato di distruzione che è archiviato presso l'ufficio di registrazione. L'ufficio di registrazione conserva i certificati di distruzione dei documenti TRÈS SECRET UE/EU TOP SECRET per un periodo di almeno dieci anni e quelli dei documenti CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET per un periodo di almeno cinque anni.
47. I documenti classificati, compresi quelli di livello RESTREINT UE/EU RESTRICTED, sono distrutti con metodi conformi alle pertinenti norme UE o equivalenti, ovvero approvati dagli Stati membri in conformità delle norme tecniche nazionali, per impedirne la ricostituzione integrale o parziale.
48. La distruzione dei supporti informatici delle ICUE è effettuata conformemente al punto 36 dell'allegato A IV.

## VII. ISPEZIONI DI SICUREZZA

### Ispezioni di sicurezza del SEAE

49. Conformemente all'articolo 15 della presente decisione, le ispezioni di sicurezza del SEAE comprendono:
- (a) ispezioni di sicurezza generali, il cui obiettivo è valutare il livello di sicurezza generale della sede centrale del SEAE, delle delegazioni dell'Unione e di tutti i locali accessori o collegati, soprattutto al fine di valutare l'efficacia delle misure di sicurezza attuate per proteggere gli interessi del SEAE in materia di sicurezza;
  - (b) ispezioni di sicurezza delle ICUE, il cui scopo è valutare, generalmente in vista di un accreditamento, l'efficacia delle misure attuate per la protezione delle ICUE nella sede centrale del SEAE e nelle delegazioni dell'Unione.

In particolare, tali ispezioni sono effettuate, tra l'altro, al fine di:

- (i) garantire il rispetto delle norme minime per proteggere le ICUE stabilite dalla presente decisione;
- (ii) sottolineare l'importanza della sicurezza e della gestione efficace del rischio presso le entità ispezionate;
- (iii) raccomandare contromisure per attenuare l'impatto specifico della perdita di riservatezza, integrità o disponibilità delle informazioni classificate; nonché
- (iv) rafforzare i programmi in corso di formazione e sensibilizzazione alla sicurezza, condotti dalle autorità di sicurezza.

### Svolgimento delle ispezioni di sicurezza e stesura dei rapporti di ispezione del SEAE

50. Le ispezioni di sicurezza del SEAE sono condotte da una squadra addetta della direzione "Sicurezza" del SEAE e, se necessario, con il sostegno di esperti in materia di sicurezza di altre istituzioni dell'UE o degli Stati membri.
- La squadra addetta all'ispezione ha accesso a tutti i luoghi in cui sono trattate ICUE, in particolare gli uffici di registrazione e i punti di presenza del CIS.
51. Le ispezioni di sicurezza del SEAE nelle delegazioni dell'Unione possono essere effettuate, ove necessario, con il sostegno dei responsabili della sicurezza presso le ambasciate degli Stati membri nei paesi terzi.
52. Prima della fine di ciascun anno civile, l'autorità di sicurezza del SEAE adotta un programma per le ispezioni di sicurezza del SEAE per l'anno successivo.
53. Ogniqualvolta sia necessario, l'autorità di sicurezza del SEAE può organizzare ispezioni di sicurezza non contemplate nel programma suddetto.

54. Al termine dell'ispezione di sicurezza le conclusioni e raccomandazioni principali sono presentate all'entità ispezionata. Successivamente, la squadra addetta all'ispezione redige un rapporto sull'ispezione. Qualora siano state proposte misure correttive e raccomandazioni, il rapporto contiene precisazioni sufficienti a sostegno delle conclusioni. Il rapporto è trasmesso all'autorità di sicurezza del SEAE e al responsabile dell'entità ispezionata.

Un regolare rapporto è stilato sotto la responsabilità dell'autorità di sicurezza della direzione "Sicurezza" del SEAE per evidenziare gli insegnamenti tratti dalle ispezioni condotte negli Stati membri durante un determinato periodo ed esaminato dal Comitato per la sicurezza del SEAE.

**Svolgimento delle ispezioni di sicurezza, e stesura dei rapporti d'ispezione, nelle agenzie e organi UE istituiti ai sensi del titolo V, capo 2, del TUE**

55. La direzione "Sicurezza" del SEAE può, se del caso, designare esperti a partecipare a squadre comuni UE che effettuano ispezioni nelle agenzie e negli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE.

**Lista di controllo delle ispezioni di sicurezza del SEAE**

56. La direzione "Sicurezza" del SEAE elabora e aggiorna la lista di controllo delle ispezioni di sicurezza per i punti da verificare nel corso di un'ispezione del SEAE. La lista è trasmessa al Comitato per la sicurezza del SEAE.
57. Le informazioni per completare la lista di controllo sono ottenute in particolare durante l'ispezione dal personale addetto alla gestione della sicurezza dell'entità ispezionata. Una volta completata con le risposte dettagliate ottenute, la lista di controllo è classificata, d'intesa con l'entità ispezionata. Essa non fa parte del rapporto di ispezione.
-

## ALLEGATO A IV

**PROTEZIONE DELLE ICUE TRATTATE NEI CIS****I. INTRODUZIONE**

1. Il presente allegato stabilisce le disposizioni di attuazione dell'articolo 8 dell'allegato A.
2. Le proprietà e i concetti seguenti in materia di garanzia di sicurezza delle informazioni (IA) sono essenziali per la sicurezza e il corretto funzionamento operativo dei sistemi di comunicazione e di informazione (CIS):

Autenticità:	garanzia che l'informazione è veritiera e proviene da fonti in buona fede
Disponibilità:	proprietà di accessibilità e utilizzabilità su richiesta di un'entità autorizzata
Riservatezza:	proprietà per cui l'informazione non è divulgata a persone, entità o procedure non autorizzate
Integrità:	proprietà di tutela della precisione e della completezza delle informazioni e delle risorse
Non disconoscibilità:	capacità di provare che un'azione o un evento sono effettivamente accaduti e non possono essere negati in seguito.

**II. PRINCIPI DI GARANZIA DI SICUREZZA DELLE INFORMAZIONI**

3. Le disposizioni esposte di seguito sono alla base della sicurezza di tutti i CIS che trattano ICUE. I requisiti d'attuazione dettagliati di queste disposizioni sono definiti nelle politiche e negli orientamenti di sicurezza in materia di IA.

**Gestione del rischio di sicurezza**

4. La gestione del rischio di sicurezza è parte integrante della definizione, dello sviluppo, del funzionamento e della manutenzione dei CIS. La gestione del rischio (valutazione, trattamento, accettazione e comunicazione) è condotta congiuntamente, nel quadro di un processo iterativo, da rappresentanti dei proprietari dei sistemi, autorità di progetto, autorità operative e autorità preposte all'approvazione di sicurezza, avvalendosi di una procedura comprovata, trasparente e ben comprensibile di valutazione del rischio. La portata del CIS e delle relative risorse è definita esplicitamente all'inizio della procedura di gestione del rischio.
5. Le autorità competenti del SEAE esaminano le potenziali minacce ai CIS e tengono aggiornate e complete le valutazioni dei rischi corrispondenti all'ambiente operativo del momento. Esse tengono costantemente aggiornate le proprie conoscenze relative alle questioni della vulnerabilità e rivedono periodicamente la valutazione di vulnerabilità alla luce dell'evoluzione dell'ambiente di tecnologia dell'informazione (TI).
6. La gestione del rischio di sicurezza è volta ad applicare una serie di misure di sicurezza che risultino in un equilibrio soddisfacente tra le esigenze degli utenti e il rischio di sicurezza residuo.
7. I requisiti, la portata e il grado di dettaglio specifici determinati dall'autorità di accreditamento di sicurezza (SAA) competente per l'accREDITAMENTO di un CIS sono commisurati al rischio valutato, tenendo conto di tutti i fattori pertinenti, tra cui il livello di classifica delle ICUE trattate nel CIS. L'accREDITAMENTO comprende una dichiarazione formale sul rischio residuo e l'accettazione di tale rischio da parte di un'autorità responsabile.

**Sicurezza lungo tutto il ciclo di vita del CIS**

8. La garanzia della sicurezza è un obbligo lungo tutto il ciclo di vita del CIS, dall'inizio al ritiro dal servizio.
9. Il ruolo e l'interazione di ciascun attore di un CIS con riferimento alla sua sicurezza è individuato per ciascuna fase del ciclo di vita.
10. Qualsiasi CIS, comprese le relative misure di sicurezza tecniche e non tecniche, è soggetto a prove di sicurezza durante il processo di accREDITAMENTO per assicurarsi che le misure di sicurezza attuate rispondano a un adeguato livello di garanzia e per verificare che sia applicato, integrato e configurato correttamente.
11. Le valutazioni, le ispezioni e le verifiche di sicurezza sono effettuate periodicamente durante il funzionamento e la manutenzione di un CIS nonché quando si verificano circostanze eccezionali.

12. La documentazione di sicurezza di un CIS evolve durante il suo ciclo di vita come parte integrante del processo di gestione dei cambiamenti e delle configurazioni.

#### **Migliori prassi**

13. Il SEAE collabora con il SGC, la Commissione e gli Stati membri per sviluppare migliori prassi di protezione delle ICUE trattate nei CIS. Gli orientamenti sulle migliori prassi stabiliscono misure di sicurezza tecniche, materiali, organizzative e procedurali per i CIS di comprovata efficacia nel combattere determinate minacce e vulnerabilità.
14. La protezione delle ICUE trattate nei CIS si avvale dell'esperienza maturata dalle entità coinvolte nell'IA all'interno e al di fuori dell'UE.
15. La diffusione e successiva attuazione delle migliori prassi favorisce il raggiungimento di un livello equivalente di garanzia di sicurezza dei vari CIS, gestiti dal SEAE, che trattano ICUE.

#### **Difesa in profondità**

16. Per attenuare il rischio per i CIS è attuata una serie di misure di sicurezza tecniche e non tecniche, organizzate come fasi multiple di difesa. Tali fasi comprendono:

- (a) *la deterrenza*: misure di sicurezza volte a scoraggiare progetti ostili di attacco ai CIS;
- (b) *la prevenzione*: misure di sicurezza volte a ostacolare o bloccare un attacco ai CIS;
- (c) *il rilevamento*: misure di sicurezza volte a scoprire un attacco ai CIS;
- (d) *la resilienza*: misure di sicurezza volte a limitare l'impatto di un attacco ad una serie minima di informazioni o risorse del CIS evitando ulteriori danni; nonché
- (e) *il ripristino*: misure di sicurezza volte a ripristinare il funzionamento in sicurezza del CIS.

Il livello di rigore e applicabilità di tali misure di sicurezza è determinato in base a una valutazione del rischio.

17. Le autorità competenti del SEAE assicurano di poter rispondere a incidenti che trascendano i limiti organizzativi e nazionali, coordinando le risposte e mettendo in comune le informazioni sui suddetti incidenti e il relativo rischio (capacità di risposta in caso di emergenza informatica).

#### **Principio di essenzialità e privilegio minimo**

18. Per evitare rischi inutili sono attuate solo le funzionalità, i dispositivi e i servizi per soddisfare i requisiti operativi.
19. Agli utenti dei CIS e alle procedure automatizzate sono forniti solo l'accesso, i privilegi o le autorizzazioni necessari allo svolgimento dei loro compiti, onde limitare i danni derivanti da incidenti, errori o uso non autorizzato delle risorse dei CIS.
20. Le procedure di registrazione effettuate dal CIS, ove necessario, sono verificate nel quadro del processo di accreditamento.

#### **Sensibilizzazione alla garanzia di sicurezza delle informazioni**

21. La sensibilizzazione ai rischi e alle misure di sicurezza disponibili è la prima linea di difesa per la sicurezza dei CIS. In particolare, tutto il personale attivo nel ciclo di vita dei CIS, compresi gli utenti, è consapevole di quanto segue:
- (a) le disfunzioni della sicurezza possono danneggiare gravemente i CIS e l'intera organizzazione;
  - (b) il potenziale danno ad altri che può derivare dall'interconnettività e dall'interdipendenza; nonché
  - (c) la responsabilità personale, e l'obbligo di rendere conto della sicurezza dei CIS secondo i rispettivi ruoli all'interno dei sistemi e delle procedure.
22. Per assicurare che le responsabilità in materia di sicurezza siano ben comprese, tutto il personale coinvolto, ivi compresi i quadri dirigenziali e gli utenti dei CIS, è tenuto a seguire corsi di formazione e sensibilizzazione all'IA.

**Valutazione e approvazione dei prodotti di sicurezza TI**

23. Il livello necessario di fiducia nelle misure di sicurezza, definito quale livello di garanzia, è determinato in base ai risultati della procedura di gestione del rischio e conformemente alle politiche e agli orientamenti di sicurezza pertinenti.
24. Il livello di garanzia è verificato tramite procedure e metodologie riconosciute internazionalmente o approvate a livello nazionale. Ciò comprende in primo luogo valutazione, controlli e verifiche.
25. I prodotti crittografici per la protezione delle ICUE sono valutati e approvati dall'autorità di approvazione degli apparati crittografici (CAA) nazionale di uno Stato membro.
26. Prima di essere raccomandati per approvazione della CAA del SEAE, conformemente all'articolo 7, paragrafo 5, della presente decisione, tali prodotti crittografici sono valutati positivamente da un secondo soggetto, ossia l'autorità di validazione qualificata (AQUA) di uno Stato membro non coinvolto nella progettazione o produzione delle attrezzature in questione. Il livello di precisione richiesto nella valutazione del secondo soggetto dipende dal livello di classifica massima previsto per le ICUE che tali prodotti devono proteggere.
27. Ove giustificato da specifici motivi operativi, il CAA del SEAE può, su raccomandazione del Comitato per la sicurezza del Consiglio, dispensare dai requisiti di cui ai punti 25 o 26 e rilasciare un'approvazione temporanea per un determinato periodo in conformità dell'articolo 7, paragrafo 5, della presente decisione.
28. Un'AQUA è una CAA di uno Stato membro che è stata accreditata in base ai criteri stabiliti dal Consiglio per procedere alla seconda valutazione dei prodotti crittografici ai fini della protezione delle ICUE.
29. L'Alto rappresentante approva una politica di sicurezza sulla qualificazione e l'approvazione dei prodotti di sicurezza TI non crittografici.

**Trasmissione nelle zone protette**

30. In deroga alle disposizioni della presente decisione, se la trasmissione di ICUE è limitata a zone protette è possibile procedere ad una distribuzione non cifrata o a una cifratura di livello inferiore in base ai risultati di una procedura di gestione del rischio e previa approvazione della SAA.

**Sicurezza dell'interconnessione dei CIS**

31. Ai fini della presente decisione, per interconnessione s'intende la connessione diretta tra due o più sistemi TI ai fini della condivisione dei dati e delle altre risorse dell'informazione (ad esempio, comunicazione) in modo unidirezionale o multidirezionale.
32. Un CIS considera inaffidabili i sistemi TI interconnessi e applica misure di protezione per controllare lo scambio d'informazioni classificate.
33. Per tutte le interconnessioni dei CIS con un altro sistema TI sono soddisfatti i requisiti di base seguenti:
  - (a) i requisiti commerciali o operativi di tali interconnessioni sono dichiarati e approvati dalle autorità competenti;
  - (b) l'interconnessione è soggetta ad una procedura di gestione del rischio e di accreditamento e richiede l'approvazione della SAA competente; nonché
  - (c) lungo il perimetro di tutti i CIS sono attuati servizi di protezione perimetrale (BPS).
34. Non vi è interconnessione tra un CIS accreditato e una rete non protetta o pubblica, ad eccezione dei casi i cui il CIS ha approvato BPS installati a tal fine tra il CIS stesso e la rete non protetta o pubblica. Le misure di sicurezza per tali interconnessioni sono esaminate dall'autorità per la garanzia di sicurezza delle informazioni (IAA) competente e approvate dalla SAA competente.

Se la rete non protetta o pubblica è usata solo come vettore e i dati sono criptati con un prodotto crittografico approvato conformemente all'articolo 7, paragrafo 5, della presente decisione, tale connessione non è considerata un'interconnessione.

35. È vietata l'interconnessione diretta o a cascata di un CIS accreditato per il trattamento di informazioni classificate TRÈS SECRET UE/EU TOP SECRET a una rete non protetta o pubblica.

#### **Supporti informatici**

36. I supporti informatici sono distrutti secondo procedure approvate dall'autorità di sicurezza del SEAE.
37. I supporti informatici sono riutilizzati, declassati o declassificati secondo la politica di sicurezza da stabilire a norma dell'articolo 7, paragrafo 2, della presente decisione.

#### **Situazioni di emergenza**

38. In deroga alle disposizioni della presente decisione, le procedure specifiche descritte di seguito possono essere applicate per un periodo limitato di tempo in casi di emergenza, come in situazioni di crisi, conflitti, guerre imminenti o già in corso o in circostanze operative eccezionali.
39. Le ICUE possono essere trasmesse, previo consenso dell'autorità competente, usando prodotti crittografici approvati per un livello di classifica inferiore o senza cifratura nel caso in cui un ritardo causerebbe un danno manifestamente maggiore di quello dovuto all'eventuale divulgazione del materiale classificato e se:
- (a) il mittente e il destinatario non hanno l'attrezzatura di cifratura necessaria o non hanno alcuna attrezzatura di cifratura; e
  - (b) il materiale classificato non può essere trasmesso in tempo utile con altri mezzi.
40. Le informazioni classificate trasmesse nelle circostanze di cui al punto 39 non recano alcun contrassegno o indicazione che le distinguano da informazioni non classificate o che possono essere protette mediante prodotti crittografici disponibili. I destinatari sono informati tempestivamente e con altri mezzi del livello di classifica.
41. In caso di ricorso al punto 39, un successivo rapporto deve essere trasmesso alla direzione "Sicurezza" del SEAE e, per il tramite di questa, al Comitato per la sicurezza del SEAE. Tale rapporto dovrà indicare almeno il mittente, il destinatario e l'originatore di tutte le ICUE.

### **III. FUNZIONI E AUTORITÀ DI GARANZIA DI SICUREZZA DELLE INFORMAZIONI**

42. Presso il SEAE sono istituite le seguenti funzioni in materia di IA. Tali funzioni non richiedono entità organizzative uniche. Esse hanno mandati separati. Tuttavia, tali funzioni, e le responsabilità ad esse collegate, possono combinarsi o integrarsi nella stessa entità organizzativa o suddividersi tra diverse entità organizzative, a condizione che si evitino conflitti interni di interessi o di mansioni.

#### **Autorità per la garanzia di sicurezza delle informazioni (IAA)**

43. L'IAA ha il compito di:
- (a) sviluppare politiche e orientamenti di sicurezza in materia di IA e monitorarne l'efficacia e la pertinenza;
  - (b) salvaguardare e gestire informazioni tecniche relative ai prodotti crittografici;
  - (c) garantire che le misure in materia di IA adottate per proteggere le ICUE rispettino le politiche pertinenti che ne disciplinano l'ammissibilità e la selezione;
  - (d) garantire che i prodotti crittografici siano selezionati nel rispetto delle politiche che ne disciplinano l'ammissibilità e la selezione;
  - (e) coordinare la formazione e la sensibilizzazione in materia di IA;
  - (f) consultare il fornitore del sistema, gli operatori della sicurezza e i rappresentanti degli utenti per quanto riguarda politiche e orientamenti di sicurezza in materia di IA; e
  - (g) assicurare la disponibilità di adeguate conoscenze tecniche nella sotto-sezione di esperti del Comitato per la sicurezza del SEAE per le questioni IA.

**Autorità TEMPEST**

44. L'Autorità TEMPEST (TA) è responsabile della conformità dei CIS con le politiche e gli orientamenti TEMPEST. Essa approva le contromisure TEMPEST per le installazioni e i prodotti per la protezione delle ICUE a un determinato livello di classifica nel suo contesto operativo.

**Autorità di approvazione degli apparati crittografici (CAA)**

45. La CAA ha il compito di assicurare che i prodotti crittografici siano conformi alla rispettiva politica in materia di crittografia. L'autorità approva un prodotto crittografico per la protezione delle ICUE a un determinato livello di classifica nel suo contesto operativo.

**Autorità di distribuzione degli apparati crittografici (CDA)**

46. La CDA ha il compito di:

- (a) gestire e rendere conto del materiale crittografico dell'UE;
- (b) assicurare che siano attuate procedure appropriate e siano stabiliti canali per rendere conto di tutto il materiale crittografico dell'UE e assicurarne il trattamento, la conservazione e la diffusione in modo sicuro; e
- (c) assicurare il trasferimento di materiale crittografico dell'UE verso o da singole persone o servizi che lo utilizzano.

**Autorità di accreditamento di sicurezza (SAA)**

47. La SAA per ciascun sistema ha il compito di:

- (a) assicurare che il CIS sia conforme alle politiche e agli orientamenti di sicurezza pertinenti, fornire una dichiarazione di approvazione del CIS per il trattamento di ICUE a un determinato livello di classifica nel suo contesto operativo, specificare i termini e le condizioni dell'accREDITamento e i criteri in base ai quali è richiesta una nuova approvazione;
- (b) stabilire un processo di accREDITamento di sicurezza, conformemente alle pertinenti politiche, definendo chiaramente le condizioni per l'approvazione dei CIS sotto la sua autorità;
- (c) definire una strategia di accREDITamento di sicurezza che stabilisce il grado di dettaglio del processo di accREDITamento commisurato al livello di garanzia richiesto;
- (d) esaminare e approvare la documentazione attinente alla sicurezza, comprese le dichiarazioni di gestione del rischio e quelle sul rischio residuo, le dichiarazioni relative ai requisiti di sicurezza specifici del sistema ("SSRS"), la documentazione relativa alla verifica dell'attuazione della sicurezza e le procedure operative di sicurezza ("SecOp"), e garantirne la conformità alle norme e politiche del SEAE in materia di sicurezza;
- (e) controllare l'attuazione di misure di sicurezza in relazione al CIS effettuando o patrocinando valutazioni, ispezioni o riesami riguardo alla sicurezza;
- (f) definire requisiti di sicurezza (ad esempio, livelli di nulla osta di sicurezza del personale) per i posti sensibili in relazione al CIS;
- (g) approvare la selezione di prodotti crittografici e TEMPEST approvati, utilizzati per garantire la sicurezza di un CIS;
- (h) approvare l'interconnessione ad altri CIS di un CIS o, se del caso, partecipare all'approvazione comune di tale interconnessione; e
- (i) consultare il fornitore del sistema, gli operatori della sicurezza e i rappresentanti degli utenti per quanto riguarda la gestione del rischio di sicurezza, in particolare il rischio residuo, nonché i termini e le condizioni della dichiarazione di approvazione.

48. La SAA del SEAE è responsabile dell'accREDITamento di tutti i CIS operanti nell'ambito di competenza del SEAE.

**Comitato di accREDITamento di sicurezza (SAB)**

49. Un SAB comune è responsabile dell'accREDITamento dei CIS nell'ambito di competenza sia della SAA del SEAE che delle SAA degli Stati membri. Esso è composto di un rappresentante SAA per ciascuno Stato membro e vi partecipa un rappresentante SAA del SGC e della Commissione. Altri soggetti con nodi su un CIS sono invitati a partecipare alle discussioni su tale sistema.

Il SAB è presieduto da un rappresentante della SAA del SEAE. Esso delibera per consenso dei rappresentanti SAA delle istituzioni, degli Stati membri e di altri soggetti con nodi sul CIS. Esso riferisce periodicamente circa le sue attività al Comitato per la sicurezza del SEAE a cui notifica tutte le dichiarazioni di accreditamento.

#### **Autorità operativa per la garanzia di sicurezza delle informazioni**

50. L'autorità operativa IA per ciascun sistema ha il compito di:

- (a) sviluppare una documentazione di sicurezza conforme alle politiche e agli orientamenti di sicurezza, in particolare la dichiarazione relativa ai requisiti di sicurezza specifici del sistema (SSRS), compresa la dichiarazione sul rischio residuo, le procedure operative di sicurezza (SecOP) e il piano crittografico nell'ambito del processo di accreditamento del CIS;
  - (b) partecipare alla selezione e alla verifica 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 e dispositivi di sicurezza TEMPEST se richiesto nell'SSRS e assicurarne l'installazione e la manutenzione in modo sicuro in cooperazione con la TA;
  - (d) controllare l'attuazione e l'applicazione delle SecOP e, ove opportuno, delegare le responsabilità di sicurezza operativa al proprietario del sistema;
  - (e) gestire e trattare prodotti crittografici, assicurando la custodia di apparati crittografici e controllati e, se richiesto, garantire la produzione di variabili crittografiche;
  - (f) procedere a verifiche dell'analisi di sicurezza e a prove, in particolare per elaborare le pertinenti relazioni sui rischi, come richiesto dalla SAA;
  - (g) fornire una formazione IA specifica del CIS;
  - (h) attuare e mettere in funzione misure di sicurezza specifiche del CIS.
-

## ALLEGATO A V

**SICUREZZA INDUSTRIALE****I. INTRODUZIONE**

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 9 dell'allegato A. Esso stabilisce disposizioni generali di sicurezza applicabili a soggetti industriali o di altra natura, in sede di negoziati precontrattuali e lungo tutto il ciclo di vita dei contratti classificati conclusi dal SEAE.
2. L'Alto rappresentante approva una politica sulla sicurezza industriale che delinea in particolare requisiti dettagliati in ordine al nulla osta di sicurezza delle imprese (FSC), alle lettere sugli aspetti di sicurezza (SAL), alle visite, alla trasmissione e al trasporto di ICUE.

**II. ELEMENTI DI SICUREZZA IN UN CONTRATTO CLASSIFICATO****Guida alle classifiche di sicurezza (SCG)**

3. Prima di indire un bando di gara o di concludere un contratto classificato, il SEAE, in quanto autorità contraente, stabilisce la classifica di sicurezza delle informazioni che devono essere fornite agli offerenti e ai contraenti, nonché la classifica di sicurezza delle informazioni che il contraente deve creare. A tal fine il SEAE mette a punto una SCG ai fini dell'esecuzione del contratto.
4. Per stabilire la classifica di sicurezza dei vari elementi di un contratto classificato si applicano i principi seguenti:
  - (a) nel redigere l'SCG, il SEAE tiene conto di tutti gli aspetti in materia di sicurezza, tra cui la classifica di sicurezza assegnata alle informazioni fornite e approvate per l'uso ai fini del contratto dall'originatore delle informazioni stesse;
  - (b) il livello generale di classifica del contratto non può essere inferiore alla classifica più elevata di uno dei suoi elementi; e
  - (c) ove opportuno, il SEAE si mette in contatto con le NSA/DSA degli Stati membri o altre autorità di sicurezza competenti interessate in caso di qualsiasi modifica nella classifica delle informazioni create dai contraenti o ad essi fornite nell'esecuzione di un contratto e di eventuali ulteriori modifiche alla SCG.

**Lettera sugli aspetti di sicurezza (SAL)**

5. I requisiti di sicurezza specifici del contratto sono indicati in una SAL. Ove opportuno, tale SAL contiene la SCG ed è parte integrante di un contratto o subcontratto classificato.
6. La SAL contiene disposizioni che impongono al contraente e/o al subcontraente di osservare le norme minime stabilite dalla presente decisione. L'inosservanza di tali norme minime può essere motivo sufficiente di estinzione del contratto.

**Istruzioni di sicurezza del programma/progetto (PSI)**

7. Secondo la portata dei programmi o dei progetti che comportano l'accesso a ICUE o il loro trattamento o la loro conservazione, l'autorità contraente incaricata della gestione del programma o del progetto può redigere specifiche istruzioni di sicurezza del programma/progetto (PSI). Le PSI richiedono l'approvazione delle NSA/DSA degli Stati membri o delle altre autorità di sicurezza competenti che partecipano al programma/progetto e possono contenere requisiti di sicurezza supplementari.

**III. NULLA OSTA DI SICUREZZA DELLE IMPRESE (FSC)**

8. La direzione "Sicurezza" del SEAE richiede alla NSA o DSA o ad altra autorità di sicurezza competente dello Stato membro interessato di concedere un FSC per indicare, in conformità delle leggi e dei regolamenti nazionali, che un soggetto industriale o di altra natura è in grado di proteggere le ICUE al livello adatto di classifica (CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET) all'interno delle proprie strutture. A un contraente o subcontraente o potenziale contraente o subcontraente non sono fornite ICUE né è consentito l'accesso ad esse finché non è stata trasmessa prova dell'FSC al SEAE.
9. Ove opportuno, il SEAE, in quanto autorità contraente, comunica all'NSA/DSA pertinente o altra autorità di sicurezza competente che è necessario un FSC in fase precontrattuale o di esecuzione del contratto. In fase precontrattuale è richiesto un FSC o un PSC laddove occorre fornire ICUE classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante il processo di presentazione delle offerte.

10. Il SEAE, in quanto autorità contraente, non assegna all'offerente selezionato un contratto classificato prima di aver ricevuto conferma dall'NSA/DSA, o da altra autorità di sicurezza competente dello Stato membro in cui ha sede il contraente o subcontraente interessato, che laddove necessario è stato rilasciato l'FSC adatto.
11. Il SEAE, in quanto autorità contraente, chiede all'NSA/DSA o ad altra autorità di sicurezza competente che ha rilasciato un FSC di essere informato in merito a informazioni negative inerenti l'FSC. In caso di subcontratto, l'NSA/DSA o altra autorità di sicurezza competente è informata di conseguenza.
12. La revoca dell'FSC da parte dell'NSA/DSA interessata o di altra autorità di sicurezza competente è motivo sufficiente per far sì che il SEAE, in quanto autorità contraente, estingua il contratto classificato o escluda l'offerente dalla gara.

#### IV. NULLA OSTA DI SICUREZZA DEL PERSONALE (PSC) PER IL PERSONALE DEI CONTRAENTI

13. Il personale che lavora per contraenti, con necessità di accedere a ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, ha ricevuto il nulla osta di sicurezza adeguato e accede a tali informazioni secondo il principio della necessità di conoscere. Per l'accesso a ICUE di livello RESTREINT UE/EU RESTRICTED non è richiesto un PSC ma deve tuttavia sussistere la necessità di conoscere.
14. Le richieste di PSC per il personale dei contraenti sono presentate all'NSA/DSA competente per l'entità interessata.
15. Il SEAE fa presente ai contraenti, che intendano assumere un cittadino di uno Stato terzo per una posizione che richiede l'accesso a ICUE, che spetta alle NSA/DSA dello Stato membro in cui è ubicata e registrata l'entità che assume stabilire se la persona interessata può accedere a tali informazioni, in conformità alla presente decisione, e confermare che l'originatore vi abbia acconsentito, prima di fornire l'accesso.

#### V. CONTRATTI O SUBCONTRATTI CLASSIFICATI

16. Qualora ad un offerente siano fornite ICUE in fase precontrattuale, l'invito a presentare offerte contiene una disposizione che impone all'offerente, che non ha presentato l'offerta o che non è stato selezionato, l'obbligo di restituire tutti i documenti classificati entro un periodo di tempo determinato.
17. Una volta aggiudicato il contratto o il subcontratto classificato, il SEAE, in quanto autorità contraente, notifica all'NSA/DSA o altra autorità di sicurezza competente del contraente o subcontraente le disposizioni di sicurezza del contratto classificato.
18. In caso di estinzione o scadenza dei suddetti contratti il SEAE, in quanto autorità contraente (e/o l'NSA/DSA o altra autorità di sicurezza competente, ove opportuno, in caso di subcontratto), ne informa immediatamente l'NSA/DSA o altra autorità di sicurezza competente dello Stato membro in cui il contraente o subcontraente ha sede.
19. Di norma, alla cessazione o scadenza del contratto o del subcontratto classificato, il contraente o subcontraente è tenuto a restituire all'autorità contraente le ICUE in suo possesso.
20. La SAL contiene disposizioni specifiche per l'eliminazione di ICUE durante l'esecuzione o alla cessazione o scadenza del contratto.
21. Se è autorizzato a conservare le ICUE alla cessazione o scadenza del contratto, il contraente o subcontraente continua a rispettare le norme minime previste dalla presente decisione nonché a proteggere la riservatezza delle ICUE.
22. Le condizioni alle quali è ammesso il subcontratto da parte del contraente sono definite nel bando di gara e nel contratto.
23. Prima di subappaltare parti di un contratto classificato il contraente ottiene il consenso del SEAE in quanto autorità contraente. Nessun subcontratto può essere aggiudicato a un soggetto industriale o di altra natura avente sede in uno Stato non membro dell'UE che non abbia concluso un accordo sulla sicurezza delle informazioni con l'UE.
24. Spetta al contraente assicurare che tutte le attività del subcontratto si svolgano secondo le norme minime previste dalla presente decisione e astenersi dal fornire ICUE a un subcontraente senza previo consenso scritto dell'autorità contraente.

25. L'autorità contraente esercita i diritti dell'originatore sulle ICUE create o trattate dal contraente o subcontraente.

#### VI. VISITE RELATIVE A CONTRATTI CLASSIFICATI

26. Se il SEAE, i contraenti o subcontraenti richiedono l'accesso ad informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei rispettivi locali per l'esecuzione di un contratto classificato, le visite sono fissate di concerto con le NSA/DSA o altre autorità di sicurezza competenti interessate. Nel contesto di progetti specifici ciò non pregiudica la prerogativa delle NSA/DSA di concordare una procedura secondo la quale tali visite possono essere fissate direttamente.
27. Tutti i visitatori dispongono di un PSC adatto e hanno una necessità di conoscere per accedere alle ICUE relative ad un contratto del SEAE.
28. I visitatori possono accedere solo alle ICUE relative all'oggetto della visita.

#### VII. TRASMISSIONE E TRASPORTO DI ICUE

29. Per la trasmissione elettronica di ICUE si applicano le pertinenti disposizioni dell'articolo 8 dell'allegato A e dell'allegato A IV.
30. In ordine al trasporto di ICUE, si applicano le pertinenti disposizioni dell'allegato A III, conformemente alle disposizioni legislative e regolamentari nazionali.
31. Per il trasporto di materiale classificato come carico, nel fissare i dispositivi di sicurezza si applicano i principi seguenti:
- (a) la sicurezza è garantita in tutte le fasi del trasporto dal luogo di origine alla destinazione finale;
  - (b) il livello di protezione attribuito ad una spedizione è determinato dal livello di classifica più elevato del materiale trasportato;
  - (c) un FSC di livello adatto è ottenuto per le società addette al trasporto, se il trasporto comporta la conservazione delle informazioni classificate nei locali dei contraenti. In ogni caso, il personale addetto alla spedizione dispone di un nulla osta di sicurezza adeguato conformemente all'allegato A, capitolo I;
  - (d) qualsiasi movimento transfrontaliero di materiale classificato CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET è subordinato a un programma di trasporto elaborato dal mittente e approvato dal SEAE, se del caso di concerto con l'NSA/DSA sia del mittente che del destinatario o con altre autorità di sicurezza competenti interessate;
  - (e) i tragitti sono effettuati, per quanto possibile, da punto a punto e sono completati quanto più rapidamente possibile secondo le circostanze;
  - (f) gli itinerari dovrebbero attraversare, per quanto possibile, unicamente Stati membri. Gli itinerari attraverso Stati diversi dagli Stati membri dovrebbero essere seguiti solo se autorizzati dal SEAE o da altra autorità di sicurezza competente degli Stati dello speditore e del destinatario.

#### VIII. TRASMISSIONE DI ICUE A CONTRAENTI SITUATI IN PAESI TERZI

32. Le ICUE sono trasmesse a contraenti e subcontraenti situati in paesi terzi che hanno un accordo di sicurezza con l'UE, secondo misure di sicurezza convenute tra il SEAE, in quanto autorità contraente, e l'NSA/DSA dello Stato terzo interessato in cui il contraente ha sede.

#### IX. TRATTAMENTO E CONSERVAZIONE DELLE INFORMAZIONI CLASSIFICATE RESTREINT UE/ EU RESTRICTED

33. Di concerto con l'NSA/DSA dello Stato membro, se opportuno, il SEAE, in quanto autorità contraente, ha diritto di procedere a visite dei locali dei contraenti/subcontraenti in forza delle disposizioni contrattuali, per verificare che siano attuate le misure di sicurezza per la protezione delle ICUE di livello RESTREINT UE/EU RESTRICTED come da contratto.

34. Nella misura in cui è necessario a norma delle disposizioni legislative e regolamentari nazionali, le NSA/DSA o qualsiasi altra autorità nazionale competente sono informate dal SEAE, in quanto autorità contraente, dei contratti o subcontratti contenenti informazioni classificate RESTREINT UE/EU RESTRICTED.
  35. Per i contratti stipulati dal SEAE contenenti informazioni classificate RESTREINT UE/EU RESTRICTED, i contraenti o subcontraenti e relativo personale non sono tenuti a possedere un FSC o un PSC.
  36. Il SEAE, in quanto autorità contraente, esamina le risposte agli inviti a presentare offerte per i contratti che richiedono l'accesso a informazioni classificate RESTREINT UE/EU RESTRICTED, a prescindere da eventuali requisiti vigenti a norma delle disposizioni legislative e regolamentari nazionali in ordine agli FSC o PSC.
  37. Le condizioni alle quali è ammesso il subcontratto da parte del contraente sono conformi ai punti 22-24.
  38. Se un contratto comporta il trattamento di informazioni classificate RESTREINT UE/EU RESTRICTED in un CIS gestito da un contraente, il SEAE, in quanto autorità contraente, garantisce che nel contratto o eventuale subcontratto siano specificati i requisiti tecnici e amministrativi necessari in ordine all'accREDITAMENTO del CIS commisurati al rischio valutato, tenendo conto di tutti i fattori pertinenti. La portata dell'accREDITAMENTO di tale CIS è concordata tra l'autorità contraente e l'NSA/DSA competente.
-

## ALLEGATO A VI

**SCAMBIO DI INFORMAZIONI CLASSIFICATE CON STATI TERZI E ORGANIZZAZIONI INTERNAZIONALI****I. INTRODUZIONE**

1. Il presente allegato stabilisce le disposizioni di attuazione dell'articolo 10 dell'allegato A.

**II. QUADRI CHE DISCIPLINANO LO SCAMBIO DI INFORMAZIONI CLASSIFICATE**

2. Il SEAE può scambiare ICUE con Stati terzi o un'organizzazione internazionale ai sensi dell'articolo 10, paragrafo 1, dell'allegato A.

Per sostenere l'AR nell'adempimento delle responsabilità di cui all'articolo 218 del trattato sul funzionamento dell'Unione europea:

- (a) il dipartimento geografico o tematico pertinente del SEAE, in consultazione con la direzione "Sicurezza" del SEAE, individua, se del caso, la necessità di scambi di ICUE a lungo termine con lo Stato terzo o l'organizzazione internazionale interessati;
  - (b) la direzione "Sicurezza" del SEAE, in consultazione con il competente dipartimento geografico del SEAE, presenta all'AR, se del caso, progetti di testi da proporre al Consiglio a norma dell'articolo 218, paragrafo 3, 5 e 6 del TFUE;
  - (c) la direzione "Sicurezza" del SEAE sostiene l'AR nella conduzione di negoziati, in coordinamento con i competenti servizi della Commissione e del Segretariato generale del Consiglio;
  - (d) In relazione ad accordi o intese con Stati terzi per la loro partecipazione a operazioni PSDC di gestione delle crisi di cui all'articolo 10, paragrafo 1, lettera c), dell'allegato A, la direzione Gestione delle crisi e pianificazione del SEAE, di concerto con i competenti servizi del SEAE, se del caso, presenta all'AR progetti di testi da proporre al Consiglio a norma dell'articolo 218, paragrafi 3, 5 e 6 del TFUE, e sostiene l'AR nella conduzione di negoziati in coordinamento con i competenti servizi del SEAE e del Segretariato generale del Consiglio.
3. Se gli accordi sulla sicurezza delle informazioni prevedono modalità tecniche di attuazione da concordare tra la direzione "Sicurezza" del SEAE, in coordinamento con la direzione "Sicurezza" della direzione generale Risorse umane e sicurezza della Commissione e il servizio di sicurezza del Segretariato generale del Consiglio, e l'autorità competente in materia di sicurezza dello Stato terzo o dell'organizzazione internazionale in questione, tali modalità tengono conto del livello di protezione stabilito dalle normative, strutture e procedure esistenti in materia di sicurezza nello Stato terzo o nell'organizzazione internazionale in questione.
  4. Qualora per il SEAE sussista la necessità a lungo termine di scambiare informazioni classificate di livello non superiore a RESTREINT UE/EU RESTRICTED con uno Stato terzo o un'organizzazione internazionale e sia stato accertato che il terzo in questione non possiede un sistema di sicurezza sufficientemente sviluppato da consentirgli di concludere un accordo sulla sicurezza delle informazioni, l'AR, previo parere favorevole unanime del Comitato per la sicurezza del SEAE e conformemente all'articolo 14, paragrafo 5, della presente decisione, può concludere un'intesa amministrativa con le autorità di sicurezza competenti dello Stato terzo o dell'organizzazione internazionale in questione.
  5. Le ICUE non sono scambiate per via elettronica con uno Stato terzo o un'organizzazione internazionale se non esplicitamente previsto dall'accordo sulla sicurezza delle informazioni o dall'intesa amministrativa.
  6. Nell'ambito di un'intesa amministrativa sullo scambio di informazioni classificate, il SEAE e lo Stato terzo o l'organizzazione internazionale designano ciascuno un ufficio di registrazione come principale punto d'ingresso e uscita delle informazioni classificate scambiate. Per il SEAE, tale ufficio è l'ufficio centrale di registrazione del SEAE.
  7. Le intese amministrative assumono di norma la forma di uno scambio di lettere.

**III. VISITE DI VALUTAZIONE**

8. Le visite di valutazione di cui all'articolo 16 della presente decisione sono effettuate di comune accordo con lo Stato terzo o l'organizzazione internazionale in questione, e valutano:

- (a) il quadro normativo applicabile per la protezione delle informazioni classificate;

- (b) eventuali aspetti specifici di leggi, regolamenti, politiche o procedure in materia di sicurezza dello Stato terzo o dell'organizzazione internazionale che possano avere un impatto sul livello massimo delle informazioni classificate che possono essere scambiate;
  - (c) le procedure e misure di sicurezza in vigore per la protezione delle informazioni classificate; e
  - (d) le procedure per il nulla osta di sicurezza per il livello delle ICUE da comunicare.
9. Non si procede allo scambio di ICUE prima che sia stata effettuata una visita di valutazione e sia stato determinato il livello al quale possono essere scambiate informazioni classificate tra le parti sulla base dell'equivalenza del livello di protezione che sarà loro assicurato.

Se, in attesa di tale visita di valutazione, l'AR è messo a conoscenza di motivi urgenti o eccezionali per scambiare informazioni classificate, il SEAE:

- (a) ottiene anzitutto il consenso scritto dell'originatore al fine di accertare l'assenza di obiezioni al loro rilascio;
- (b) consulta l'autorità di sicurezza del SEAE, che può decidere di rilasciarle previo parere favorevole unanime degli Stati membri rappresentati in seno al Comitato per la sicurezza del SEAE.

Qualora il SEAE non sia in grado di stabilire l'originatore, l'autorità di sicurezza del SEAE si assume la responsabilità dell'originatore, previo parere favorevole unanime del Comitato per la sicurezza del SEAE.

#### IV. FACOLTÀ DI COMUNICARE ICUE A STATI TERZI O ORGANIZZAZIONI INTERNAZIONALI

10. Qualora esista un quadro normativo in conformità dell'articolo 10, paragrafo 1, dell'allegato A per lo scambio di informazioni classificate con uno Stato terzo o un'organizzazione internazionale, la decisione del SEAE di comunicare ICUE a uno Stato terzo o un'organizzazione internazionale è presa dall'autorità di sicurezza del SEAE che può delegare tale autorizzazione ad alti funzionari del SEAE o ad altre persone poste sotto la sua autorità.
11. Se l'originatore delle informazioni classificate da comunicare, compresi gli originatori del materiale di base in esse eventualmente presente, non è il SEAE, quest'ultimo ne ottiene anzitutto il consenso scritto al fine di accertare l'assenza di obiezioni al rilascio. Se il SEAE non è in grado di stabilire l'originatore, l'autorità di sicurezza del SEAE si assume la responsabilità dell'originatore, previo parere favorevole unanime degli Stati membri rappresentati in seno al Comitato per la sicurezza del SEAE.

#### V. COMUNICAZIONE ECCEZIONALE AD HOC DI ICUE

12. In assenza di uno dei quadri di cui all'articolo 10, paragrafo 1, dell'allegato A, e se gli interessi dell'UE o di uno o più Stati membri richiedono il rilascio di ICUE per motivi politici, operativi o urgenti, queste possono essere eccezionalmente comunicate a uno Stato terzo o un'organizzazione internazionale una volta intraprese le azioni che seguono.

La direzione "Sicurezza" del SEAE, dopo aver accertato che le condizioni di cui al punto 11 sono soddisfatte:

- (a) per quanto possibile, verifica con le autorità di sicurezza dello Stato terzo o dell'organizzazione internazionale in questione che le loro normative, strutture e procedure in materia di sicurezza siano tali da garantire che le ICUE ad essi comunicate saranno protette secondo criteri non meno rigorosi di quelli previsti nella presente decisione;
  - (b) invita il Comitato per la sicurezza del SEAE a formulare un parere, sulla base delle informazioni disponibili, circa la fiducia che può essere riposta in normative, strutture e procedure in materia di sicurezza dello Stato terzo o dell'organizzazione internazionale a cui devono essere comunicate le ICUE;
  - (c) consulta l'autorità di sicurezza del SEAE, che può decidere di rilasciarle previo parere favorevole unanime degli Stati membri rappresentati in seno al Comitato per la sicurezza del SEAE.
13. In assenza di uno dei quadri di cui all'articolo 10, paragrafo 1, dell'allegato A, il terzo in questione si impegna per iscritto a proteggere le ICUE in modo appropriato.
-

## APPENDICE A

## DEFINIZIONI

Ai fini della presente decisione si intende per:

“accettazione del rischio”, la decisione di accettare la permanenza di un rischio residuo in seguito al trattamento del rischio;

“accreditamento”, il processo che porta a una dichiarazione formale dell'autorità di accreditamento di sicurezza (SAA) con la quale un sistema è abilitato a funzionare con un determinato livello di classifica, in particolari condizioni di sicurezza nel proprio ambiente operativo e ad un livello di rischio accettabile, in base al presupposto dell'attuazione di una serie convenuta di misure di sicurezza a livello tecnico, materiale, organizzativo e procedurale;

“autorità di sicurezza designata”, (DSA), autorità, che fa capo all'autorità di sicurezza nazionale (NSA) di uno Stato membro, incaricata di comunicare ai soggetti industriali o di altra natura la linea politica nazionale riguardo a tutti gli aspetti della sicurezza industriale e di fornire guida e assistenza nell'attuazione della medesima. La funzione della DSA può essere espletata dall'NSA o da qualsiasi altra autorità competente;

“autorizzazione di accesso a ICUE”, l'autorizzazione rilasciata dall'autorità di sicurezza del SEAE ai sensi della presente decisione previo rilascio di un PSC da parte delle autorità competenti di uno Stato membro, attestante che una persona può avere accesso a ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore) e a una data stabilita, a condizione che sia stata accertata la sua necessità di conoscere — cfr. l'articolo 2 dell'allegato A I;

“certificato di nulla osta di sicurezza personale” (PSCC), il certificato rilasciato da una autorità competente attestante che una persona è in possesso del nulla osta di sicurezza e detiene un PSC valido e in cui figura il livello di ICUE (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore) cui detta persona può accedere, la data di validità del relativo PSC e la data di scadenza del certificato stesso;

“ciclo di vita del CIS”, l'intera durata dell'esistenza di un CIS che comprende inizio, concezione, pianificazione, analisi dei requisiti, progettazione, sviluppo, verifica, attuazione, funzionamento, manutenzione e disattivazione;

“compromissione di ICUE”, la divulgazione totale o parziale di ICUE a persone o entità non autorizzate — cfr. articolo 8, paragrafo 2;

“comunicazione del rischio”, consiste nel promuovere la sensibilizzazione ai rischi tra le comunità di utenti del CIS, informando di tali rischi le autorità di approvazione e riferendo sugli stessi alle autorità operative;

“contraente”, una persona fisica o giuridica avente la capacità giuridica di sottoscrivere un contratto;

“contratto classificato”, un contratto di fornitura di beni, di esecuzione di lavori o di prestazione di servizi, stipulato fra il SEAE e un contraente, la cui esecuzione richiede o implica l'accesso o la produzione di ICUE;

“declassamento”, una riduzione del livello di classifica di sicurezza;

“declassificazione”, la soppressione di qualsiasi classifica di sicurezza;

“detentore”, una persona debitamente autorizzata con una necessità di conoscere stabilita, che detiene un elemento di ICUE ed è di conseguenza responsabile della sua protezione;

“dichiarazione relativa ai requisiti di sicurezza specifici” (SSRS), una serie di principi di sicurezza vincolanti da osservare e di dettagliati requisiti di sicurezza da attuare su cui si fonda il processo di certificazione e di accreditamento dei CIS;

“difesa in profondità”, l'applicazione di una serie di misure di sicurezza organizzate come fasi multiple di difesa;

“documento”, qualsiasi informazione registrata, a prescindere dalla sua forma o dalle sue caratteristiche materiali;

“garanzia di sicurezza delle informazioni” nel campo dei sistemi di comunicazione e informazione, la fiducia nel fatto che tali sistemi proteggeranno le informazioni che trattano e funzioneranno nel modo dovuto e a tempo debito sotto il controllo degli utenti legittimi. Una IA efficace garantisce gli adeguati livelli di riservatezza, integrità, disponibilità, non disconoscibilità e autenticità. L'IA si basa su una procedura di gestione del rischio — cfr. articolo 8, paragrafo 1, dell'allegato A;

“gestione delle informazioni classificate”, l'applicazione di misure amministrative intese a controllare le ICUE per tutto il loro ciclo di vita al fine di integrare le misure previste agli articoli 5, 6 e 8 e in tal modo contribuire a scoraggiare, scoprire e porre rimedio ai casi di compromissione o perdita intenzionale o accidentale di tali informazioni. Dette misure riguardano in particolare la creazione, la registrazione, la riproduzione, la traduzione, il trasporto, il trattamento, la conservazione e la distruzione di ICUE — cfr. articolo 7, paragrafo 1, dell'allegato A;

“guida alle classifiche di sicurezza” (SCG), il documento che illustra gli elementi di un programma o di un contratto classificati e precisa i livelli di classifica di sicurezza applicabili. L'SCG può essere integrata per tutta la durata del programma o del contratto e gli elementi informativi possono essere riclassificati o declassati; laddove è presente una SCG, questa fa parte della SAL — cfr. allegato A V, sezione II;

“indagine di sicurezza”, le procedure investigative condotte dall'autorità competente di uno Stato membro conformemente alle disposizioni legislative e regolamentari nazionali volte ad accertare l'inesistenza di informazioni negative note sul conto di una persona che osterebbero alla concessione in suo favore di un PSC nazionale o UE per accedere a ICUE fino a un livello specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore);

“informazioni classificate UE” (ICUE), qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri — cfr. articolo 2, lettera f);

“interconnessione”, ai fini della presente decisione, è la connessione diretta tra due o più sistemi TI ai fini della condivisione dei dati e delle altre risorse dell'informazione (ad esempio comunicazione) in modo unidirezionale o multidirezionale — cfr. allegato A IV, punto 31;

“istruzioni di sicurezza del programma/progetto” (PSI), un elenco delle procedure di sicurezza che sono applicate a un programma/progetto specifico per uniformare le stesse procedure di sicurezza. Detto elenco può essere riveduto per tutta la durata del programma/progetto;

“lettera sugli aspetti di sicurezza” (SAL), il pacchetto di condizioni contrattuali specifiche emesso dall'autorità contraente, che è parte integrante di un contratto classificato implicante l'accesso o la creazione di ICUE e in cui sono individuati i requisiti di sicurezza o gli elementi del contratto che richiedono una protezione di sicurezza — cfr. allegato A V, sezione II;

“materiale”, qualsiasi documento o elemento di macchinario o attrezzatura, sia sotto forma di prodotto finito, sia in corso di lavorazione;

“minaccia”, la causa potenziale di un incidente indesiderato che può recar danno a un'organizzazione o a uno dei sistemi in uso; tali minacce possono essere accidentali o intenzionali (dolose) e sono caratterizzate da elementi di minaccia, potenziali obiettivi e metodologie d'attacco;

“nulla osta di sicurezza delle imprese (FSC)”, una decisione amministrativa di un'NSA o DSA, secondo la quale un'impresa è in grado, sotto il profilo della sicurezza, di offrire un adeguato livello di protezione alle ICUE di un determinato livello di classifica di sicurezza e il personale di detta impresa che deve accedere alle ICUE ha debitamente ottenuto il nulla osta di sicurezza ed è stato istruito sui pertinenti requisiti di sicurezza necessari per l'accesso e la protezione delle ICUE;

“nulla osta di sicurezza personale” (PSC) per l'accesso alle ICUE, una dichiarazione rilasciata da un'autorità competente di uno Stato membro fatta al termine di un'indagine di sicurezza condotta dalle autorità competenti di uno Stato membro e attestante che una persona può avere accesso a ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), e a una data stabilita, a condizione che sia stata accertata la sua necessità di conoscere; la persona così descritta è in possesso del “nulla osta di sicurezza”;

“operazione PSDC”, un'operazione di gestione militare o civile delle crisi ai sensi del titolo V, capo 2, del TUE;

“originatore”, l'istituzione, l'agenzia o l'organo dell'UE, lo Stato membro, lo Stato terzo o l'organizzazione internazionale sotto la cui autorità sono state create e/o introdotte nelle strutture dell'UE informazioni classificate;

“procedura di gestione del rischio”, l'intera procedura di individuazione, controllo e riduzione al minimo di eventi incerti che possono incidere sulla sicurezza di un'organizzazione o di un qualsiasi sistema in uso. Contempla tutte le attività correlate al rischio, tra cui la valutazione, il trattamento, l'accettazione e la comunicazione;

“procedure operative di sicurezza” (SecOP), la descrizione delle modalità da adottare per l'attuazione della politica di sicurezza, delle procedure operative da seguire e delle responsabilità del personale;

“prodotti crittografici (crypto)”, algoritmi crittografici, moduli hardware e software crittografici e prodotti comprendenti dettagli di attuazione e documentazione associata e materiale di codifica;

“registrazione”, l'applicazione di procedure che registrano il ciclo di vita delle informazioni, ivi comprese la diffusione e la distruzione — cfr. allegato A, parte III, punto 21;

“rischio”, la possibilità che una data minaccia sfrutti le vulnerabilità interne ed esterne di un'organizzazione o di uno qualsiasi dei sistemi da essa utilizzati, arrecando pertanto danno all'organizzazione o ai suoi beni materiali o immateriali. È calcolato come una combinazione tra le probabilità del verificarsi delle minacce e il loro impatto;

“rischio residuo”, il rischio che resta una volta attuate le misure di sicurezza, dato che non tutte le minacce possono essere neutralizzate né tutte le vulnerabilità eliminate;

“risorsa”, qualsiasi cosa che ha valore per un'organizzazione, le sue operazioni economiche e la loro continuità, comprese le risorse dell'informazione che sostengono la missione dell'organizzazione;

“sicurezza del personale”, l'applicazione di misure volte a garantire che l'accesso alle ICUE sia consentito solo alle persone che:

- hanno necessità di conoscere;
- per l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, hanno ottenuto il nulla osta di sicurezza del livello adatto o sono in altro modo debitamente autorizzate in virtù delle loro funzioni secondo le disposizioni legislative e regolamentari nazionali; e
- sono state informate delle proprie responsabilità in materia —

cfr. articolo 5, paragrafo 1, dell'allegato A;

“sicurezza industriale”, l'applicazione di misure che assicurino la protezione delle ICUE da parte di contraenti o subcontraenti in sede di negoziati precontrattuali e lungo tutto il ciclo di vita dei contratti classificati — cfr. articolo 9, paragrafo 1, dell'allegato A;

“sicurezza materiale”, l'applicazione di misure di protezione materiali e tecniche volte ad impedire l'accesso non autorizzato alle ICUE — cfr. articolo 6 dell'allegato A;

“sistema di comunicazione e informazione” (CIS), ogni sistema che consente il trattamento delle informazioni in forma elettronica. Un sistema di comunicazione e informazione comprende l'insieme delle risorse necessarie al suo funzionamento, ivi compresi l'infrastruttura, l'organizzazione, il personale e le risorse dell'informazione — cfr. articolo 8, paragrafo 2, dell'allegato A;

“soggetto industriale o di altra natura”, un soggetto che si occupa della fornitura di beni, della esecuzione di lavori o della prestazione di servizi; può trattarsi di un soggetto del settore industriale, commerciale, di servizi, scientifico, di ricerca, didattico o di sviluppo, ovvero di un lavoratore autonomo;

“subcontratto classificato”, un contratto di fornitura di beni, di esecuzione di lavori o di prestazione di servizi, stipulato fra un contraente del SEAE e un altro contraente (ossia il subcontraente), la cui esecuzione richiede o implica l'accesso o la produzione di ICUE;

“TEMPEST”, l'indagine, lo studio e il controllo delle radiazioni elettromagnetiche che possono compromettere le informazioni e le misure per eliminarle;

“trattamento” delle ICUE, qualsiasi azione di cui possono essere oggetto le ICUE nel loro ciclo di vita. Ciò comprende la loro creazione, elaborazione, trasporto, declassamento, declassificazione e distruzione. In relazione al CIS il trattamento comprende anche raccolta, visualizzazione, trasmissione e conservazione;

“trattamento del rischio”, consiste nel mitigare, rimuovere, ridurre (tramite un'opportuna combinazione di misure tecniche, materiali, organizzative o procedurali), trasferire o controllare il rischio;

“valutazione del rischio”, l'identificazione delle minacce e delle vulnerabilità e l'effettuazione delle relative analisi del rischio, ossia l'analisi della probabilità e dell'impatto;

“violazione”, l'atto o l'omissione di una persona contrari alle norme di sicurezza contenute nella presente decisione e/o alle politiche o agli orientamenti di sicurezza che precisano le misure necessarie per la sua attuazione;

“vulnerabilità”, una debolezza di qualsiasi tipo che una o più minacce possono sfruttare. La vulnerabilità può derivare da un'omissione o essere legata ad una debolezza nei controlli in termini di rigore, completezza o coerenza e può essere di natura tecnica, procedurale, materiale, organizzativa od operativa.

---