II

(Atti non legislativi)

DECISIONI

DECISIONE DEL CONSIGLIO

del 31 marzo 2011

sulle norme di sicurezza per la protezione delle informazioni classificate UE

(2011/292/UE)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 240, paragrafo 3,

vista la decisione 2009/937/UE del Consiglio, del 1º dicembre 2009, relativa all'adozione del suo regolamento interno [1], in particolare l'articolo 24,

considerando quanto segue:

(1) Al fine di sviluppare le attività del Consiglio in tutti i settori che richiedono il trattamento di informazioni classificate, è opportuno porre in essere un sistema di sicurezza globale per la protezione delle informazioni classificate riguardante il Consiglio, il suo segretariato generale e gli Stati membri.

(2) La presente decisione dovrebbe applicarsi qualora il Consiglio, i suoi organi preparatori e il segretariato generale del Consiglio (SGC) trattino informazioni classificate UE (ICUE).

(3) In conformità delle disposizioni legislative e regolamentari nazionali e nella misura richiesta per il funzionamento del Consiglio, gli Stati membri dovrebbero rispettare la presente decisione nei casi in cui le loro autorità competenti, il loro personale e i loro contraenti trattino ICUE, affinché tutti possano avere la certezza che un livello equivalente di protezione è assicurato alle ICUE.

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

(5) Il Consiglio sottolinea l'importanza di associare, ove opportuno, il Parlamento europeo ed altri istituzioni, agenzie, organi o uffici dell'UE a principi, regole e norme per proteggere le informazioni classificate che sono necessari per salvaguardare gli interessi dell'Unione e dei suoi Stati membri.

(6) Le agenzie e gli organi dell'UE istituiti ai sensi del titolo V, capo 2, del trattato sull'Unione europea, Europol ed Eurojust applicano, nel contesto della rispettiva organizzazione interna, i principi di base e le norme minime contenute nella presente decisione per proteggere le ICUE, secondo quanto previsto nei rispettivi atti istitutivi.

(7) Le operazioni di gestione delle crisi stabilite ai sensi del titolo V, capo 2, del TUE ed il relativo personale applicano le norme di sicurezza adottate dal Consiglio per proteggere le ICUE.

(8) I rappresentanti speciali dell'UE e i membri delle loro squadre applicano le norme di sicurezza adottate dal Consiglio per proteggere le ICUE.

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

(10) La presente decisione lascia impregiudicate le pratiche vigenti negli Stati membri per quanto riguarda l'informazione dei Parlamenti nazionali in merito alle attività dell'Unione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Oggetto, ambito di applicazione e definizioni

1. La presente decisione stabilisce i principi fondamentali e le norme minime di sicurezza per proteggere le ICUE.

[1] GU L 325 dell'11.12.2009, pag. 35.

2. I principi fondamentali e le norme minime di sicurezza si applicano al Consiglio e all'SGC e sono rispettati dagli Stati membri conformemente alle loro rispettive disposizioni legislative e regolamentari nazionali, affinché tutti possano avere la certezza che un livello equivalente di protezione è assicurato alle ICUE.

3. Ai fini della presente decisione, si applicano le definizioni che figurano nell'appendice A.

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. Le autorità competenti garantiscono 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. Il Consiglio approva una politica di sicurezza sulla creazione di ICUE che comprende una guida pratica per la classificazione.

Articolo 4

Protezione di informazioni classificate

1. Le ICUE sono protette conformemente alla presente decisione.

2. Il detentore di qualsiasi 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 dell'Unione europea, il Consiglio e l'SGC proteggono 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.

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

Articolo 5

Gestione del rischio di sicurezza

1. Il rischio per le ICUE è gestito 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 conformemente ai principi fondamentali e alle norme minime contenuti nella presente decisione, e ad applicare tali misure secondo il concetto di difesa in profondità definito all'appendice A. L'efficacia di tali misure è valutata costantemente.

2. Le misure di sicurezza 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 a livello locale della minaccia di attività dolose e/o criminali, compreso lo spionaggio, il sabotaggio e il terrorismo.

3. I piani di emergenza tengono conto della necessità di proteggere le ICUE in situazioni di emergenza onde evitare l'accesso non autorizzato, la divulgazione o la perdita di integrità o di disponibilità.

4. I piani di continuità operativa comprendono misure di prevenzione e recupero per minimizzare l'impatto di disfunzioni o incidenti gravi nel trattamento e nella conservazione delle ICUE.

Articolo 6

Attuazione della presente decisione

1. Se necessario il Consiglio, su raccomandazione del Comitato per la sicurezza, approva politiche di sicurezza che esplicitano le misure destinate ad attuare la presente decisione.

2. Il Comitato per la sicurezza può stabilire, per quanto di sua competenza, orientamenti di sicurezza intesi a integrare o sostenere la presente decisione e ogni eventuale politica di sicurezza approvata dal Consiglio.

Articolo 7

Sicurezza del personale

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

— hanno necessità di conoscere,

— hanno ottenuto il nulla osta di sicurezza del livello adatto, ove opportuno, e

— sono state informate delle proprie responsabilità in materia.

2. Le procedure per il nulla osta di sicurezza del personale sono intese a determinare se una persona, in considerazione della sua lealtà, onestà e affidabilità, può essere autorizzata ad accedere alle ICUE.

3. Tutte le persone in seno all'SGC le cui mansioni possono richiedere l'accesso a ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore dispongono del nulla osta di sicurezza del livello adatto prima di poter accedere a dette ICUE. La procedura per il nulla osta di sicurezza del personale relativa ai funzionari e agli altri agenti dell'SGC figura nell'allegato I.

4. Il personale degli Stati membri di cui all'articolo 14, paragrafo 3, le cui mansioni possono richiedere l'accesso a ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore dispone del nulla osta di sicurezza del livello adatto o è in altro modo debitamente autorizzato in virtù delle sue funzioni, secondo le disposizioni legislative e regolamentari nazionali, prima di poter accedere a dette ICUE.

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

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

Articolo 8

Sicurezza materiale

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, per scoraggiare, ostacolare e scoprire azioni non autorizzate e per consentire la segregazione del personale per quanto riguarda il loro 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 10, 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 II e approvate dall'autorità di sicurezza competente.

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 II.

Articolo 9

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 7, 8 e 10 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 copiatura, la traduzione, il trasporto 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 dell'SGC e degli Stati membri 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 ed i locali in cui sono trattate o conservate ICUE sono sottoposti a ispezioni periodiche da parte dell'autorità di sicurezza competente.

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 10, paragrafo 6;

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 10, paragrafo 6; o

ii) in tutti gli altri casi, secondo quanto prescritto dall'autorità di sicurezza competente, conformemente alle pertinenti misure di protezione dell'allegato III.

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

Articolo 10

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» 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. La presente decisione si applica ai sistemi di comunicazione e informazione che trattano ICUE (CIS).

3. I CIS trattano le ICUE conformemente al concetto di IA.

4. Tutti i CIS 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 le modalità seguenti:

a) la riservatezza delle informazioni classificate di livello SECRET UE/EU SECRET e superiore è protetta mediante prodotti crittografici approvati dal Consiglio in quanto autorità di approvazione degli apparati crittografici (CAA), su raccomandazione del Comitato per la sicurezza;

b) la riservatezza delle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o RESTREINT UE/EU RESTRICTED è protetta mediante prodotti crittografici approvati dal segretario generale del Consiglio («il segretario generale») in quanto CAA, su raccomandazione del Comitato per la sicurezza.

In deroga alla lettera b), all'interno dei sistemi nazionali degli Stati membri la riservatezza delle ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o RESTREINT UE/EU RESTRICTED può essere protetta mediante prodotti crittografici approvati dalla CAA di uno Stato membro.

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 IV.

8. Le autorità competenti dell'SGC e degli Stati membri stabiliscono rispettivamente 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. Per ciascun sistema le autorità competenti dell'SGC e degli Stati membri stabiliscono rispettivamente:

a) un'autorità di accreditamento di sicurezza (SAA);

b) un'autorità operativa IA.

10. Le disposizioni di attuazione del presente articolo figurano nell'allegato IV.

Articolo 11

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. Detti contratti non contemplano l'accesso alle informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET.

2. L'SGC 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 che abbia concluso un accordo o un'intesa amministrativa conformemente all'articolo 12, paragrafo 2, lettere a) o b).

3. In quanto autorità contraente, l'SGC, 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.

4. L'autorità di sicurezza nazionale (NSA), l'autorità di sicurezza designata (DSA) o qualsiasi altra autorità nazionale competente di ciascuno Stato membro assicura, per quanto possibile ai sensi delle disposizioni legislative e regolamentari nazionali, che i contraenti e i subcontraenti registrati nel suo territorio adottino le misure adeguate per proteggere le ICUE nei negoziati precontrattuali e nell'esecuzione di un contratto classificato.

5. L'NSA, la DSA o qualsiasi altra autorità di sicurezza competente di ciascuno Stato membro assicura, conformemente alle disposizioni legislative e regolamentari nazionali, che i contraenti e i subcontraenti registrati nel territorio dello Stato membro in questione, partecipanti a contratti o subcontratti classificati che richiedono l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nelle loro strutture dispongano, nell'esecuzione di tali contratti o nella fase precontrattuale, di un nulla osta di sicurezza delle imprese (FSC) del livello di classifica adatto.

6. 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 ottiene un nulla osta di sicurezza personale (PSC) 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 I.

7. Le disposizioni di attuazione del presente articolo figurano nell'allegato V.

Articolo 12

Scambio di informazioni classificate con Stati terzi ed organizzazioni internazionali

1. Qualora il Consiglio ravvisi la necessità di scambiare ICUE con uno Stato terzo o un'organizzazione internazionale, è posto in essere a tal fine un quadro appropriato.

2. Per stabilire tale quadro e definire disposizioni reciproche sulla protezione delle informazioni classificate scambiate:

a) il Consiglio conclude accordi sulle procedure di sicurezza per scambiare e proteggere informazioni classificate («accordi sulla sicurezza delle informazioni»); o

b) il segretario generale può pattuire intese amministrative ai sensi del punto17 dell'allegato VI laddove la classifica delle ICUE da comunicare non supera di norma il livello RESTREINT UE/EU RESTRICTED.

3. Gli accordi sulla sicurezza delle informazioni o le intese amministrative di cui al paragrafo 2 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.

4. La decisione di comunicare ad uno Stato terzo o ad un'organizzazione internazionale ICUE originate dal Consiglio è presa dal Consiglio 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. Se l'originatore delle informazioni classificate che si desiderano comunicare non è il Consiglio, l'SGC chiede anzitutto il consenso scritto dell'originatore. Se è impossibile stabilire l'originatore, il Consiglio si assume la responsabilità dell'originatore.

5. Sono organizzate visite di valutazione per accertare l'efficacia delle misure di sicurezza poste in essere in uno Stato terzo o un'organizzazione internazionale al fine di proteggere le ICUE fornite o scambiate.

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

Articolo 13

Violazione della sicurezza e compromissione di ICUE

1. La violazione della sicurezza è conseguenza di un atto o omissione di una persona contrario alle norme di sicurezza contenute nella presente decisione.

2. La compromissione si verifica quando, in seguito a una violazione della sicurezza, la ICUE sono state diffuse in tutto o in parte a persone non autorizzate.

3. Qualsiasi violazione o sospetta violazione della sicurezza è immediatamente riferita all'autorità di sicurezza competente.

4. Qualora sia noto o vi siano ragionevoli motivi di ritenere che vi sia stata compromissione o perdita di ICUE, l'autorità di sicurezza competente adotta tutte le misure adeguate secondo le pertinenti disposizioni legislative e regolamentari al fine di:

a) informare l'originatore;

b) assicurare che personale non direttamente interessato alla violazione indaghi sul caso per accertare i fatti;

c) valutare i potenziali danni agli interessi dell'UE o degli Stati membri;

d) adottare i provvedimenti opportuni per impedire che i fatti si ripetano; e

e) informare le autorità competenti delle misure adottate.

5. Ogni persona responsabile di una violazione delle norme di sicurezza contenute nella presente decisione è passibile di azione disciplinare secondo le disposizioni legislative e regolamentari applicabili. Ogni persona responsabile della compromissione o della perdita di ICUE è passibile di sanzioni disciplinari e/o azioni legali secondo le disposizioni legislative, normative e regolamentari applicabili.

Articolo 14

Responsabilità dell'attuazione

1. Il Consiglio adotta tutte le misure necessarie per garantire la coerenza globale nell'applicazione della presente decisione.

2. Il segretario generale adotta tutte le misure necessarie per garantire che, nel trattamento o nella conservazione di ICUE o di qualsiasi altra informazione classificata, i funzionari e gli altri agenti dell'SGC, il personale distaccato presso l'SGC ed i contraenti dell'SGC applichino la presente decisione nei locali usati dal Consiglio e in seno all'SGC, compresi gli uffici di collegamento negli Stati terzi.

3. Gli Stati membri adottano tutte le misure adeguate, secondo le rispettive disposizioni legislative e regolamentari nazionali, per garantire che, nel trattamento o nella conservazione di ICUE, la presente decisione sia rispettata:

a) dal personale delle Rappresentanze permanenti degli Stati membri presso l'Unione europea e dai delegati nazionali che partecipano a sessioni del Consiglio o a riunioni dei suoi organi preparatori o che prendono parte ad altre attività del Consiglio;

b) dagli altri membri del personale delle amministrazioni nazionali degli Stati membri, incluso il personale distaccato presso tali amministrazioni, che prestino servizio sul territorio degli Stati membri o all'estero;

c) dalle altre persone negli Stati membri debitamente autorizzate in virtù delle loro funzioni ad avere accesso ad ICUE; e

d) dai contraenti degli Stati membri, nel territorio degli Stati membri o all'estero.

Articolo 15

Organizzazione della sicurezza nel Consiglio

1. Nell'ambito del suo ruolo di garante della coerenza globale nell'applicazione della presente decisione, il Consiglio approva:

a) gli accordi di cui all'articolo 12, paragrafo 2, lettera a);

b) le decisioni che autorizzano la comunicazione di ICUE a Stati terzi ed organizzazioni internazionali;

c) un programma di ispezione annuale proposto dal segretario generale e raccomandato dal Comitato per la sicurezza per ispezionare i servizi e i locali degli Stati membri e delle agenzie e organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, nonché Europol ed Eurojust ed effettuare visite di valutazione negli Stati terzi e nelle organizzazioni internazionali al fine di accertare l'efficacia delle misure attuate per la protezione delle ICUE; e

d) le politiche di sicurezza di cui all'articolo 6, paragrafo 1.

2. Il segretario generale è l'autorità di sicurezza dell'SGC. In tale veste il segretario generale:

a) attua la politica di sicurezza del Consiglio e la sottopone a riesame periodico;

b) coordina con le NSA degli Stati membri tutte le questioni di sicurezza relative alla protezione di informazioni classificate pertinenti per le attività del Consiglio;

c) fornisce ai funzionari e altri agenti dell'SGC un PSC dell'UE conformemente all'articolo 7, paragrafo 3, prima che possa essere loro accordato l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore;

d) ordina, ove opportuno, indagini su compromissioni o perdite, accertate o sospette, di informazioni classificate detenute o originate dal Consiglio e chiede alle autorità di sicurezza competenti di partecipare a tali indagini;

e) compie ispezioni periodiche dei dispositivi di sicurezza per la protezione delle informazioni classificate nei locali dell'SGC;

f) compie ispezioni periodiche dei dispositivi di sicurezza per la protezione delle ICUE nelle agenzie e negli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, in Europol, Eurojust, nonché nelle operazioni di gestione delle crisi previste ai sensi del titolo V, capo 2, del TUE nonché da parte dei Rappresentanti speciali dell'UE (RSUE) e dei membri delle loro squadre;

g) compie, insieme e d'accordo con l'NSA interessata, ispezioni periodiche dei dispositivi di sicurezza per la protezione delle ICUE all'interno dei servizi e dei locali degli Stati membri;

h) coordina le misure di sicurezza con le autorità competenti degli Stati membri responsabili della protezione delle informazioni classificate e, se del caso, con Stati terzi o organizzazioni internazionali, anche per quanto riguarda la natura delle minacce alla sicurezza delle ICUE e i relativi mezzi di protezione;

i) pattuisce le intese amministrative di cui all'articolo 12, paragrafo 2, lettera b); e

j) effettua visite di valutazione iniziali e periodiche presso Stati terzi o organizzazioni internazionali al fine di accertare l'efficacia delle misure attuate per la protezione delle ICUE messe a loro disposizione o con essi scambiate.

Il servizio di sicurezza dell'SGC è a disposizione del segretario generale per assisterlo nell'ambito di tali competenze.

3. Ai fini dell'attuazione dell'articolo 14, paragrafo 3 gli Stati membri dovrebbero:

a) designare un'NSA responsabile dei dispositivi di sicurezza per proteggere le ICUE affinché:

i) le ICUE detenute da qualsiasi servizio, organo o agenzia nazionale, pubblico o privato, sul territorio nazionale o all'estero, siano protette conformemente alla presente decisione;

ii) i dispositivi di sicurezza per la protezione delle ICUE siano ispezionati regolarmente;

iii) tutte le persone impiegate in un'amministrazione nazionale o da un contraente cui può essere concesso l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore abbiano ottenuto il nulla osta di sicurezza adeguato o siano in altro modo debitamente autorizzate in virtù delle rispettive funzioni conformemente alle disposizioni legislative e regolamentari nazionali;

iv) siano istituiti programmi di sicurezza, se necessario, per minimizzare il rischio di compromissione o perdita delle ICUE;

v) gli aspetti di sicurezza connessi con la protezione di ICUE siano coordinati con altre autorità nazionali competenti, comprese quelle menzionate nella presente decisione; e

vi) sia data risposta alle opportune richieste di nulla osta di sicurezza provenienti dalle agenzie e dagli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, da Europol, Eurojust, nonché dalle operazioni di gestione delle crisi stabilite ai sensi del titolo V, capo 2, del TUE e dagli RSUE e dalle loro squadre.

Le NSA sono elencate nell'appendice C;

b) assicurare che le loro autorità competenti forniscano informazioni e consulenza ai rispettivi governi, e attraverso questi al Consiglio, circa la natura delle minacce per la sicurezza delle ICUE ed i mezzi per proteggersi da tali minacce.

Articolo 16

Comitato per la sicurezza

1. È istituito un Comitato per la sicurezza. Esso esamina e valuta ogni questione relativa alla sicurezza nell'ambito di applicazione della presente decisione e formula, ove opportuno, raccomandazioni per il Consiglio.

2. Il Comitato per la sicurezza è composto di rappresentanti delle NSA degli Stati membri e vi partecipa un rappresentante della Commissione e del servizio europeo per l'azione esterna. Esso è presieduto dal segretario generale o dal suo delegato designato. Esso si riunisce secondo le istruzioni del Consiglio, o a richiesta del segretario generale o di unNSA.

Possono essere invitati a parteciparvi rappresentanti delle agenzie e degli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, nonché di Europol ed Eurojust quando vi si discutono questioni che li riguardano.

3. Il Comitato per la sicurezza organizza le sue attività in modo da essere in grado di formulare raccomandazioni su questioni specifiche in materia di sicurezza. Esso istituisce una sotto-sezione di esperti per gli aspetti IA ed altre sotto-sezioni ove necessario. Esso redige il mandato di tali sotto-sezioni e ne riceve le relazioni di attività corredate, ove opportuno, di raccomandazioni per il Consiglio.

Articolo 17

Sostituzione di precedenti decisioni

1. La presente decisione abroga e sostituisce la decisione 2001/264/CE del Consiglio, del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio [1].

2. Tutte le ICUE classificate conformemente alla decisione 2001/264/CE continuano ad essere protette conformemente alle pertinenti disposizioni della presente decisione.

Articolo 18

Entrata in vigore

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

Fatto a Bruxelles, addì 31 marzo 2011.

Per il Consiglio
Il presidente
VÖLNER P.

[1] GU L 101 dell'11.4.2001, pag. 1.

ALLEGATI

ALLEGATO I

Sicurezza del personale

ALLEGATO II

Sicurezza materiale

ALLEGATO III

Gestione delle informazioni classificate

ALLEGATO IV

Protezione delle ICUE trattate nei CIS

ALLEGATO V

Sicurezza industriale

ALLEGATO VI

Scambio di informazioni classificate con Stati terzi ed organizzazioni internazionali

ALLEGATO I

SICUREZZA PERSONALE

I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 7. Esso stabilisce in particolare i criteri 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. In tutto il presente allegato, eccettuato laddove la distinzione è pertinente, il termine «nulla osta di sicurezza personale» si riferisce a un nulla osta di sicurezza personale nazionale (PSC nazionale) e/o a un nulla osta di sicurezza personale UE (PSC UE), definiti nell'appendice A.

II. AUTORIZZAZIONE DI ACCESSO ALLE ICUE

3. 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; e

   c) sia stata istruita sulle norme e le procedure di sicurezza per la protezione delle ICUE ed abbia riconosciuto la propria responsabilità in materia di protezione di tali informazioni.

4. Ciascuno Stato membro e l'SGC individuano all'interno delle loro 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.

III REQUISITI RELATIVI AL NULLA OSTA DI SICUREZZA PERSONALE

5. Dopo aver ricevuto una richiesta debitamente autorizzata, alle NSA o altre autorità nazionali competenti spetta assicurare che siano svolte le indagini di sicurezza sui loro cittadini che chiedono di accedere ad informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore. Le norme in materia di indagini sono conformi alle disposizioni legislative e regolamentari nazionali.

6. Qualora la persona interessata risieda nel territorio di un altro Stato membro o di uno Stato terzo, le autorità nazionali competenti richiedono della collaborazione dell'autorità competente dello Stato di residenza conformemente alle disposizioni legislative e regolamentari nazionali. Gli Stati membri si assistono reciprocamente nello svolgimento di indagini di sicurezza conformemente alle disposizioni legislative e regolamentari nazionali.

7. Ove consentito dalle disposizioni legislative e regolamentari nazionali, le NSA o altre autorità nazionali competenti possono svolgere indagini su persone che non sono cittadini dello Stato in questione che chiedono di accedere ad informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore. Le norme in materia di indagini sono conformi alle disposizioni legislative e regolamentari nazionali.

Criteri delle indagini di sicurezza

8. La lealtà, l'onestà e l'affidabilità di una persona ai fini della concessione di un PSC per l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono accertate mediante un'indagine di sicurezza. L'autorità nazionale competente effettua una valutazione generale basandosi sui risultati di tale indagine di sicurezza. Il risultato negativo su singoli elementi non costituisce necessariamente motivo di rifiuto del PSC. I criteri principali applicati a tal fine dovrebbero includere, per quanto possibile ai sensi delle disposizioni legislative e regolamentari nazionali, l'esame per determinare se la persona in questione:

   a) ha commesso o tentato di commettere atti di spionaggio, terrorismo, sabotaggio, tradimento o sedizione, ovvero ha cospirato con altri, o si è resa complice e ha istigato altri a commettere tali atti;

   b) è o è stata associata di spie, terroristi, sabotatori o di persone fondatamente sospettate di esserlo, ovvero associata di rappresentanti di organizzazioni o di Stati stranieri, compresi i servizi di intelligence stranieri, che possono costituire una minaccia per la sicurezza dell'UE e/o degli Stati membri, a meno che tale associazione non sia stata autorizzata per lo svolgimento delle sue funzioni ufficiali;

c) è o è stata membro di organizzazioni che, con mezzi violenti, sovversivi o altrimenti illegali, tentano inter alia di rovesciare il governo di uno Stato membro o di cambiarne l'ordine costituzionale o la forma o le politiche di governo;

d) fiancheggia o ha fiancheggiato una delle organizzazioni di cui alla lettera c), ovvero è o è stata strettamente associata con membri di tali organizzazioni;

e) ha deliberatamente occultato, distorto o falsificato informazioni importanti, soprattutto se pregnanti per la sicurezza, o ha deliberatamente mentito nel compilare un questionario sulla sicurezza del personale o durante un colloquio sulla sicurezza;

f) è stata condannata per uno o più reati;

g) ha una storia di alcolismo, di uso di droghe illecite e/o abuso di droghe lecite;

h) è o è stata coinvolta in comportamenti che possono renderla vulnerabile a ricatti o pressioni;

i) con parole o fatti ha dato prova di essere disonesta, sleale, inaffidabile o di non meritare fiducia;

j) ha violato gravemente o ripetutamente norme di sicurezza; o ha tentato di compiere ovvero ha compiuto azioni non autorizzate nell'ambito dei sistemi di comunicazione e informazione;

k) può essere esposta a pressioni (ad esempio per il fatto di essere in possesso della cittadinanza di uno o più Stati non membri dell'UE o tramite familiari o associati stretti che potrebbero essere vulnerabili nei confronti di servizi di intelligence stranieri, gruppi terroristici o altre organizzazioni o singoli sovversivi, i cui fini possono minacciare gli interessi dell'UE e/o degli Stati membri in materia di sicurezza).

9. Ove opportuno e conformemente alle disposizioni regolamentari e legislative nazionali, la storia clinica e finanziaria di una persona può essere considerata rilevante nell'indagine di sicurezza.

10. Ove opportuno e conformemente alle disposizioni regolamentari e legislative nazionali, nell'indagine di sicurezza possono essere considerati rilevanti anche il carattere, la condotta e la situazione del coniuge, del convivente o di un familiare stretto.

Requisiti di indagine per l'accesso alle ICUE

Concessione iniziale di un PSC

11. Il PSC iniziale per l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET si basa su un'indagine di sicurezza che considera almeno gli ultimi cinque anni o, se più breve, il periodo che intercorre tra i 18 anni di età e l'inizio delle indagini e che comprende i seguenti elementi:

a) compilazione di un questionario nazionale sulla sicurezza del personale per il livello di ICUE a cui la persona interessata può chiedere di avere accesso; una volta compilato, tale questionario è trasmesso all'autorità di sicurezza competente;

b) controllo di identità/cittadinanza/nazionalità: sono verificati il luogo e la data di nascita della persona in questione e ne è controllata l'identità. È stabilita la sua cittadinanza e/o nazionalità, passata e presente; si verifica, tra l'altro se, a causa di una residenza precedente o di associazioni avute in passato può sussistere una vulnerabilità a pressioni esercitate da fonti straniere; e

c) controllo delle iscrizioni a livello locale e nazionale: sono verificate le iscrizioni di sicurezza nazionale e il casellario giudiziale centrale, se esistente, e/o altre registrazioni comparabili dello Stato e della polizia. Sono verificate le iscrizioni effettuate dalle autorità di contrasto con giurisdizione nel luogo in cui la persona in questione ha risieduto o ha lavorato.

12. Il PSC iniziale per l'accesso a informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET si basa su un'indagine di sicurezza che considera almeno gli ultimi dieci anni o, se più breve, il periodo che intercorre tra i 18 anni di età e l'inizio delle indagini. Se sono condotti i colloqui di cui alla lettera e), le indagini riguardano almeno gli ultimi sette anni o, se più breve, il periodo che intercorre tra i 18 anni di età e l'inizio delle indagini. Oltre ai criteri di cui al punto 8, prima di concedere un PSC di livello TRÈS SECRET UE/EU TOP SECRET sono esaminati, per quanto possibile ai sensi delle disposizioni legislative e regolamentari nazionali, gli elementi seguenti, che possono essere esaminati anche prima di rilasciare un PSC di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, laddove le disposizioni legislative e regolamentari nazionali lo richiedano:

a) situazione finanziaria: sono reperite le informazioni sulla situazione patrimoniale della persona per accertare se sussiste una qualsiasi vulnerabilità a pressioni straniere o nazionali a causa di gravi difficoltà finanziarie o per scoprire ricchezze inspiegabili;

b) istruzione: sono reperite le informazioni per appurare il tipo d'istruzione ricevuta dalla persona a scuola, all'università o in altri istituti frequentati a partire dal diciottesimo anno di età o per un periodo giudicato congruo dall'autorità che svolge l'indagine;

c) lavoro: sono reperite le informazioni sull'attuale impiego e su quelli precedenti, utilizzando fonti quali le registrazioni relative alla carriera lavorativa, i rapporti sulle prestazioni o sull'efficienza e i datori di lavoro o i superiori gerarchici;

d) servizio di leva: se applicabile, sono verificati il servizio prestato nelle forze armate e il tipo di congedo; e

e) colloqui: laddove previsto e ammesso ai sensi della legislazione nazionale, la persona in questione è sottoposta ad uno o più colloqui. I colloqui si tengono anche con altre persone che sono in grado di dare una valutazione imparziale dei trascorsi, dell'attività, lealtà, onestà e affidabilità della persona in questione. Quando è prassi nazionale chiedere alla persona oggetto delle indagini referenze, le persone citate nelle referenze sono sottoposte a un colloquio, salvo che vi siano buoni motivi per non procedervi.

13. Se necessario e conformemente alle disposizioni legislative e regolamentari nazionali, possono essere svolte indagini supplementari per elaborare tutte le pertinenti informazioni disponibili sulla persona in questione e per circostanziare o confutare le informazioni negative.

Rinnovo di un PSC

14. Dopo la concessione iniziale di un PSC e sempre che la persona abbia prestato servizio ininterrottamente presso un'amministrazione nazionale o l'SGC e continui ad avere bisogno di accedere alle ICUE, il PSC è riesaminato ai fini del rinnovo a intervalli non superiori a cinque anni per un nulla osta di livello TRÈS SECRET UE/EU TOP SECRET e a dieci anni per nulla osta di livello SECRET UE/EU SECRET e CONFIDENTIEL UE/EU CONFIDENTIAL, con effetto dalla data di comunicazione dell'esito dell'ultima indagine di sicurezza su cui si basavano. Tutte le indagini di sicurezza per il rinnovo del PSC considerano il periodo intercorso dalla precedente indagine.

15. Per il rinnovo del PSC, si esaminano gli elementi descritti ai punti 11 e 12.

16. Le richieste di rinnovo sono presentate tempestivamente, tenendo conto del tempo necessario per le indagini di sicurezza. Tuttavia, se l'NSA competente o altra autorità nazionale competente ha ricevuto la pertinente richiesta di rinnovo e il corrispondente questionario sulla sicurezza del personale prima della scadenza del PSC e le indagini di sicurezza necessarie non sono ultimate, se consentito dalle disposizioni legislative e regolamentari nazionali l'autorità nazionale competente può prorogare la validità del PSC fino a dodici mesi. Se al termine di questo periodo di dodici mesi l'indagine di sicurezza non è ancora ultimata, la persona in questione è assegnata soltanto a incarichi che non richiedono un PSC.

Procedure in materia di PSC presso l'SGC

17. Per i funzionari e altri agenti dell'SGC, l'autorità di sicurezza dell'SGC 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.

18. Se viene a conoscenza di informazioni rilevanti per l'indagine di sicurezza relativa a una persona che ha chiesto un PSC UE, l'SGC le comunica all'NSA competente in conformità delle pertinenti disposizioni legislative e regolamentari.

19. Al termine dell'indagine di sicurezza l'NSA competente ne comunica l'esito all'autorità di sicurezza dell'SGC usando il formato standard per la corrispondenza previsto dal Comitato per la sicurezza.

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 dell'SGC che ha il potere di nomina può rilasciare un PSC UE alla persona interessata e autorizzare l'accesso alle ICUE fino al livello adatto e a una data determinata;

b) qualora dall'indagine di sicurezza non emerga tale garanzia, l'autorità dell'SGC che ha il potere di nomina ne informa la persona interessata la quale può chiedere di essere ascoltata dall'autorità che ha il potere di nomina. 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, un PSC UE non può essere concesso.

20. L'indagine di sicurezza e relativi risultati sono soggetti alle pertinenti disposizioni legislative e regolamentari vigenti nello Stato membro in questione, ivi comprese quelle relative ai ricorsi. Le decisioni dell'autorità dell'SGC che ha il potere di nomina 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 ([1]) («statuto e regime applicabile»).

21. La garanzia su cui è basato un PSC UE in corso di validità copre qualsiasi incarico della persona interessata all'interno dell'SGC o della Commissione.

22. Se il periodo di servizio di una persona non inizia entro dodici mesi dalla comunicazione dell'esito dell'indagine di sicurezza all'autorità dell'SGC che ha il potere di nomina o se vi è un'interruzione del servizio di dodici mesi, durante il quale la persona non ha occupato un posto presso l'SGC o l'amministrazione di uno Stato membro, tale esito è sottoposto all'NSA competente affinché questa confermi se resta valido e pertinente.

23. Se viene a conoscenza di informazioni concernenti un rischio di sicurezza posto da una persona in possesso di un PSC UE valido, l'SGC le comunica all'NSA competente in conformità alle pertinenti disposizioni legislative e regolamentari. Se un'NSA comunica all'SGC il ritiro della garanzia fornita in conformità al punto 19, lettera a) per una persona in possesso di un PSC UE valido, l'autorità dell'SGC che ha il potere di nomina può chiederle chiarimenti che è in grado di fornire conformemente alle sue disposizioni legislative e regolamentari nazionali. Se le informazioni negative sono confermate il PSC UE è ritirato 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.

24. La decisione di ritiro di un PSC UE ad un funzionario o altro agente dell'SGC e, se opportuno, i relativi motivi sono comunicati alla persona interessata la quale può chiedere di essere ascoltata dall'autorità che ha il potere di nomina. 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 dell'autorità dell'SGC che ha il potere di nomina sono soggette a ricorso in conformità allo statuto e al regime applicabile.

25. Gli esperti nazionali distaccati presso l'SGC per un posto che richiede un PSC UE presentano all'autorità di sicurezza dell'SGC un PSC nazionale valido per l'accesso alle ICUE prima di assumere l'incarico.

Registrazioni dei PSC

26. Ogni Stato membro e l'SGC conservano rispettivamente le registrazioni dei PSC nazionali e dei PSC UE concessi per l'accesso alle ICUE. Nelle registrazioni figurano almeno 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.

27. L'autorità di sicurezza competente 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 nazionale per l'accesso alle ICUE o del PSC UE e la data di scadenza del certificato stesso.

Esenzioni dall'obbligo del PSC

28. L'accesso alle ICUE negli Stati membri da parte di persone debitamente autorizzate in virtù delle loro funzioni è determinato in conformità delle disposizioni legislative e regolamentari nazionali; tali persone sono istruite sugli obblighi di sicurezza riguardo alla protezione delle ICUE.

IV. FORMAZIONE E SENSIBILIZZAZIONE ALLA SICUREZZA

29. Tutte le persone alle quali è stato concesso un PSC attestano per iscritto di aver compreso gli obblighi di protezione delle ICUE e le conseguenze che possono verificarsi se le ICUE risultano compromesse. Lo Stato membro e l'SGC, a seconda dei casi, conservano una registrazione di tale attestazione scritta.

30. Tutte le persone che sono autorizzate ad avere accesso alle 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 esse ritengono sospetto o inusuale.

31. 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.

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

V. CIRCOSTANZE ECCEZIONALI

32. Se consentito dalle disposizioni legislative e regolamentari nazionali un nulla osta di sicurezza del personale, concesso da un'autorità nazionale competente di uno Stato membro per accedere a informazioni nazionali classificate, può temporaneamente consentire, in attesa della concessione di un PSC nazionale per accedere alle ICUE, l'accesso di funzionari nazionali alle ICUE fino al livello equivalente specificato nella tabella di equivalenza che figura nell'appendice B, laddove questo accesso temporaneo sia richiesto nell'interesse dell'UE. Se le disposizioni legislative e regolamentari nazionali non consentono tale accesso temporaneo alle ICUE, le NSA ne informano il Comitato per la sicurezza.

33. Per motivi di urgenza, se debitamente giustificati nell'interesse del servizio e in attesa che sia ultimata l'indagine di sicurezza nel suo insieme, l'autorità dell'SGC che ha il potere di nomina, 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 dell'SGC per accedere alle ICUE per una funzione specifica. 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 dall'SGC.

34. 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 alle ICUE ad un 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 nazionale o di un PSC UE in corso di validità;

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 dall'autorità competente; e

g) 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.

35. 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.

36. 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, gli Stati membri e il segretario generale 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 stato data.

37. 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.

38. Il Comitato per la sicurezza è informato dei casi in cui si ricorre alla procedura descritta ai punti 36 e 37.

39. Laddove le disposizioni legislative e regolamentari nazionali di uno Stato membro stabiliscano norme più rigorose in ordine a autorizzazioni temporanee, incarichi provvisori, accesso singolo o di emergenza delle persone in questione a informazioni classificate, le procedure previste nella presente sezione sono attuate soltanto entro i limiti fissati dalle pertinenti disposizioni legislative e regolamentari nazionali.

40. Il Comitato per la sicurezza riceve una relazione annuale sul ricorso alle procedure stabilite nella presente sezione.

VI. PARTECIPAZIONE ALLE SESSIONI DEL CONSIGLIO

41. Fatto salvo il punto 28, le persone che devono partecipare a sessioni del Consiglio o a riunioni degli organi preparatori del Consiglio, 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 delegati il PSCC o altra prova di PSC è trasmesso dalle autorità competenti al Servizio di sicurezza dell'SGC o, in via eccezionale, può essere presentato dal delegato stesso. Se del caso, può essere usato un elenco di nomi consolidato che comprovi il PSC.

42. Se per ragioni di sicurezza il PSC nazionale per l'accesso alle ICUE è ritirato a una persona i cui compiti richiedono la partecipazione a sessioni del Consiglio o a riunioni degli organi preparatori del Consiglio, l'autorità competente ne informa l'SGC.

VII. ACCESSO POTENZIALE ALLE ICUE

43. 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.

44. 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, sono informati riguardo alle procedure di sicurezza in materia di protezione delle ICUE e istruiti riguardo agli obblighi di protezione delle informazioni loro affidate.

ALLEGATO II

SICUREZZA MATERIALE

I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 8. Esso stabilisce i 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 segregazione del personale per quanto riguarda l'accesso alle ICUE in base alla loro necessità di conoscere e, in caso, ai loro nulla osta di sicurezza;

   c) scoraggiando, ostacolando e scoprendo azioni non autorizzate; e

   d) impedendo o ritardando l'ingresso fraudolento o con la forza di intrusi.

II. REQUISITI E MISURE DI SICUREZZA MATERIALE

3. Le misure di sicurezza materiale sono selezionate in base alla valutazione della minaccia effettuata dalle autorità competenti. L'SGC e gli Stati membri applicano le rispettive procedure di gestione del rischio per proteggere le ICUE nei loro 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; e

   d) 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. L'autorità di sicurezza competente, nell'applicare il concetto di difesa in profondità, 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 e 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 centralinista, 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; e

   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. L'autorità competente può essere autorizzata a 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 competente 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.

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 in 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).

    Nella presente decisione tutti i riferimenti alle zone amministrative e alle zone protette, ivi comprese le zone protette tecnicamente, si intendono altresì come riferimenti agli equivalenti nazionali.

13. L'autorità di sicurezza competente 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 dall'autorità competente; e

    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 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.

17. Le zone protette che vengono protette 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. Le chiavi sono controllate in conformità della sezione VI;

    b) tutte le persone o 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 competente. Dette ispezioni sono inoltre effettuate dopo qualsiasi ingresso non autorizzato, effettivo o sospettato; e

    d) tali zone sono prive di linee di comunicazione, 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 competente 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 stabiliscano:

    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 persone 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 competente 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 III, punti da 28 a 40 e si sia impegnato ad osservare le misure compensative stabilite nelle istruzioni di sicurezza emesse dall'autorità di sicurezza competente 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 competente.

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; o

c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore:

i) trasporti le ICUE in conformità dell'allegato III, punti da 28 a 40;

ii) si sia impegnato ad osservare le misure compensative stabilite nelle istruzioni di sicurezza emesse dall'autorità di sicurezza competente per garantire che le ICUE siano protette dall'accesso di persone non autorizzate;

iii) tenga le ICUE sempre sotto il proprio controllo; e

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, secondo uno 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;

o

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 III.

VI. CONTROLLO DELLE CHIAVI E DELLE COMBINAZIONI USATE PER PROTEGGERE LE ICUE

30. L'autorità di sicurezza competente 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 hanno necessità di conoscerle. Le combinazioni dei contenitori di sicurezza e delle camere blindate in cui sono conservate ICUE sono modificate:

a) in caso di sostituzione del personale che conosce la combinazione;

b) in caso di effettiva o sospetta compromissione;

c) se una serratura è stata oggetto di manutenzione o riparazione; e

d) almeno ogni dodici mesi.

ALLEGATO III

GESTIONE DI INFORMAZIONI CLASSIFICATE

I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 9. 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 iniziale delle informazioni.

4. Il livello di classifica delle ICUE è stabilito conformemente all'articolo 2, paragrafo 2 decisione e con riferimento alla politica di sicurezza che deve essere approvata ai sensi dell'articolo 3, paragrafo 3.

5. La classifica di sicurezza è chiaramente e correttamente indicata, indipendentemente dal fatto che le ICUE siano in forma cartacea, orale, elettronica o in altra forma.

6. 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.

7. 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.

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. 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

Contrassegni

10. Oltre ad uno dei contrassegni di classifica di sicurezza di cui all'articolo 2, paragrafo 2, 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;

d) se del caso, la data o un evento specifico a seguito dei quali possono essere declassate o declassificate.

Contrassegni di classifica abbreviati

11. 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.

12. 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

13. 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 SECRET UE/EU SECRET o superiore, se devono essere distribuiti in più copie, recano un numero di copia sul ciascuna pagina.

14. Qualora non sia possibile applicare il punto 13 alle ICUE, sono adottate altre misure appropriate conformemente agli orientamenti di sicurezza che devono essere stabiliti a norma dell'articolo 6, paragrafo 2.

Declassamento e declassificazione delle ICUE

15. 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.

16. L'SGC riesamina periodicamente le ICUE in suo possesso per accertare che il livello di classifica sia ancora applicabile. L'SGC predispone 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 che le informazioni saranno automaticamente declassate o declassificate e se le informazioni sono state contrassegnate di conseguenza.

III. REGISTRAZIONE DI ICUE A FINI DI SICUREZZA

17. Per tutte le entità organizzative nell'SGC e nelle amministrazioni nazionali degli Stati membri, nelle quali sono trattate ICUE è identificato un ufficio di registrazione competente che provvede affinché le ICUE siano trattate conformemente alla presente decisione. Gli uffici di registrazione sono costituiti come zone protette definite nell'allegato II.

18. Ai fini della presente decisione, per registrazione a fini di sicurezza («registrazione») si intende l'applicazione di procedure che registrano il ciclo di vita dei materiali, ivi comprese la diffusione e la distruzione.

19. Tutti i materiali classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore sono registrati in uffici di registrazione dedicati quando entrano o lasciano un'entità organizzativa.

20. L'ufficio centrale di registrazione dell'SGC tiene un registro di tutte le informazioni classificate comunicate dal Consiglio e dall'SGC a Stati terzi e organizzazioni internazionali e di tutte le informazioni classificate pervenute da Stati terzi o organizzazioni internazionali.

21. Nel caso di un CIS, le procedure di registrazione possono essere eseguite mediante procedure interne allo stesso CIS.

22. Il Consiglio approva una politica di sicurezza per la registrazione delle ICUE a fini di sicurezza.

Uffici di registrazione TRÈS SECRET UE/EU TOP SECRET

23. Negli Stati membri e nell'SGC è designato un ufficio di registrazione che funge da autorità centrale ricevente e trasmittente per le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET. Per il trattamento delle informazioni a fini di registrazione possono essere designati, se necessario, uffici dipendenti.

24. 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'esplicito accordo di quest'ultimo.

IV. RIPRODUZIONE E TRADUZIONE DI DOCUMENTI CLASSIFICATI UE

25. I documenti di livello TRÈS SECRET UE/EU TOP SECRET possono essere riprodotti o tradotti solo previo consenso scritto dell'originatore.

26. 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.

27. Le misure di sicurezza applicabili al documento originale si applicano alle copie e alle traduzioni.

V. TRASPORTO DI ICUE

28. Il trasporto di ICUE è soggetto alle misure di protezione menzionate nei punti da 30 a 40. Se le ICUE sono trasportate con mezzi elettronici, e in deroga all'articolo 9, paragrafo 4, le misure di protezione di seguito descritte possono essere integrate da opportune contromisure tecniche prescritte dall'autorità di sicurezza competente per minimizzare il rischio di perdita o di compromissione.

29. Le autorità di sicurezza competenti dell'SGC e degli Stati membri impartiscono istruzioni sul trasporto delle ICUE in conformità della presente decisione.

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

30. 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.

31. 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 in una busta protetta recante unicamente il nome del destinatario.

All'interno dell'UE

32. Le ICUE trasportate tra edifici o locali all'interno dell'UE sono racchiuse in plichi in modo da proteggerle da divulgazione non autorizzata.

33. 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 II;

ii) le ICUE non siano aperte durante il trasporto né lette in luoghi pubblici;

iii) le persone siano istruite sulle 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 6, paragrafo 2.

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.

34. 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 33 è trasportato come carico da società di vettori commerciali conformemente all'allegato V.

35. 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

36. Le ICUE trasportate dall'UE al territorio di uno Stato terzo sono racchiuse in plichi in modo da proteggerle da divulgazione non autorizzata.

37. Il trasporto di informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIALSECRET e UE/EU SECRET dall'UE al territorio di uno Stato terzo 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 II;

iv) le ICUE non siano aperte durante il trasporto né lette in luoghi pubblici; e

v) le persone siano istruite sulle loro responsabilità in materia di sicurezza.

38. Il trasporto di informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET comunicate dall'UE a uno Stato terzo o a un'organizzazione internazionale è conforme alle pertinenti disposizioni previste in un accordo sulla sicurezza delle informazioni o un' intesa amministrativa in conformità dell'articolo 12, paragrafo 2, lettere a) o b).

39. Le informazioni classificate RESTREINT UE/EU RESTRICTED possono essere trasportate anche con servizi postali o servizi di corriere commerciale.

40. Il trasporto di informazioni classificate TRÈS SECRET UE/EU TOP SECRET dall'UE al territorio di uno Stato terzo è effettuato con corriere militare o valigia diplomatica.

VI. DISTRUZIONE DI ICUE

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

42. I documenti soggetti a registrazione ai sensi dell'articolo 9, paragrafo 2 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.

43. 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 fino al livello di classifica del documento da distruggere.

44. 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.

45. 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.

46. La distruzione dei supporti informatici delle ICUE è effettuata conformemente all'allegato IV, punto 36.

VII. ISPEZIONI E VISITE DI VALUTAZIONE

47. Il termine «ispezione» è di seguito usato per designare:

a) ogni ispezione conformemente all'articolo 9, paragrafo 3 e all'articolo 15, paragrafo 2, lettere e), f) e g); o

b) ogni visita di valutazione conformemente all'articolo 12, paragrafo 5;

intesa a valutare l'efficacia delle misure attuate per proteggere le ICUE.

48. Le ispezioni si effettuano tra l'altro al fine di:

a) garantire il rispetto delle norme minime per proteggere le ICUE stabilite dalla presente decisione;

b) sottolineare l'importanza della sicurezza e della gestione efficiente del rischio presso le entità ispezionate;

c) raccomandare contromisure per attenuare l'impatto specifico della perdita di riservatezza, integrità o disponibilità delle informazioni classificate; e

d) rafforzare i programmi in corso di formazione e sensibilizzazione alla sicurezza, condotti dalle autorità di sicurezza.

49. Prima della fine di ogni anno civile, il Consiglio adotta il programma di ispezione di cui all'articolo 15, paragrafo 1, lettera c), per l'anno successivo. Le date effettive delle singole ispezioni sono determinate di concerto con l'agenzia o l'organo dell'UE, lo Stato membro, lo Stato terzo o l'organizzazione internazionale interessati.

Svolgimento delle ispezioni

50. Le ispezioni sono effettuate per verificare le pertinenti norme, regolamentazioni e procedure dell'entità ispezionata e per verificare se le prassi dell'entità sono conformi ai principi fondamentali e alle norme minime stabilite dalla presente decisione e alle disposizioni che disciplinano lo scambio di informazioni classificate con detta entità.

51. Le ispezioni si svolgono in due fasi. Prima dell'ispezione si organizza una riunione preparatoria, se necessario, con l'entità in questione. Dopo tale riunione preparatoria la squadra addetta all'ispezione predispone, di concerto con detta entità, un programma di ispezione particolareggiato riguardante tutti i settori della sicurezza. 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.

52. Le ispezioni presso le amministrazioni nazionali degli Stati membri sono condotte sotto la responsabilità di una squadra comune SGC/Commissione, in piena collaborazione con i funzionari dell'entità ispezionata.

53. Le ispezioni presso Stati terzi e organizzazioni internazionali sono condotte sotto la responsabilità di una squadra comune SGC/Commissione, in piena collaborazione con i funzionari dello Stato terzo o dell'organizzazione internazionale oggetto dell'ispezione.

54. Le ispezioni delle agenzie e degli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, nonché di Europol ed Eurojust sono condotte dal Servizio di sicurezza dell'SGC con l'assistenza di esperti dell'NSA sul cui territorio l'agenzia o l'organo ha sede. La direzione della Sicurezza della Commissione europea (DSCE) può essere associata qualora effettui regolarmente scambi di ICUE con l'agenzia o l'organo in questione.

55. Per le ispezioni delle agenzie e degli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, nonché di Europol ed Eurojust, degli Stati terzi e delle organizzazioni internazionali si chiedono assistenza e contributi di esperti delle NSA secondo intese particolareggiate convenute con il Comitato per la sicurezza.

Rapporti di ispezione

56. Al termine dell'ispezione le conclusioni e raccomandazioni principali sono presentate all'entità ispezionata. Si stila in seguito il rapporto d'ispezione sotto la responsabilità dell'autorità di sicurezza dell'SGC (Servizio di sicurezza). Qualora siano state proposte misure correttive e raccomandazioni, il rapporto contiene precisazioni sufficienti a sostegno delle conclusioni. Il rapporto è trasmesso all'autorità competente dell'entità ispezionata.

57. Per le ispezioni condotte nelle amministrazioni nazionali degli Stati membri:

a) il progetto di rapporto d'ispezione è trasmesso all'NSA interessata affinché verifichi che sia materialmente corretto e che non contenga informazioni classificate di livello superiore a RESTREINT UE/EU RESTRICTED;

b) a meno che l'NSA dello Stato membro in questione chieda di non effettuare la distribuzione generale, i rapporti d'ispezione sono distribuiti ai membri del Comitato per la sicurezza e alla DSCE; il rapporto è classificato al livello RESTREINT UE/EU RESTRICTED;

Un regolare rapporto è stilato sotto la responsabilità dell'autorità di sicurezza dell'SGC (Servizio di sicurezza) per evidenziare gli insegnamenti tratti dalle ispezioni condotte negli Stati membri durante un determinato periodo ed esaminato dal Comitato per la sicurezza.

58. Per le visite di valutazione presso gli Stati terzi e le organizzazioni internazionali, il rapporto è distribuito al Comitato per la sicurezza e alla DSCE. Il rapporto è classificato almeno al livello RESTREINT UE/EU RESTRICTED. Eventuali misure correttive sono verificate durante una successiva visita di controllo e riferite al Comitato per la sicurezza.

59. Per le ispezioni delle agenzie e degli organi dell'UE istituiti ai sensi del titolo V, capo 2, del TUE, nonché di Europol ed Eurojust i rapporti di ispezione sono distribuiti ai membri del Comitato per la sicurezza e alla DSCE. Il progetto di rapporto di ispezione è trasmesso all'agenzia o all'organo interessato affinché verifichi che sia materialmente corretto e che non contenga informazioni classificate di livello superiore a RESTREINT UE/EU RESTRICTED. Eventuali misure correttive sono verificate durante una successiva visita di controllo e riferite al Comitato per la sicurezza.

60. L'autorità di sicurezza dell'SGC procede regolarmente a ispezioni delle entità organizzative nell'SGC ai fini indicati al punto 48.

Lista di controllo delle ispezioni

61. L'autorità di sicurezza dell'SGC (Servizio di sicurezza) elabora e aggiorna la lista di controllo delle ispezioni di sicurezza per i punti da verificare nel corso di un'ispezione. La lista è trasmessa al Comitato per la sicurezza.

62. Le informazioni per compilare la lista di controllo sono ottenute in particolare durante l'ispezione dal personale addetto alla gestione della sicurezza dell'entità ispezionata. Una volta compilata con le risposte dettagliate, la lista di controllo è classificata, d'intesa con l'entità ispezionata. Essa non fa parte del rapporto di ispezione.

ALLEGATO IV

PROTEZIONE DELLE ICUE TRATTATE NEI CIS

I. INTRODUZIONE

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

2. Le proprietà e i concetti seguenti in materia di IA sono essenziali per la sicurezza e il corretto funzionamento operativo dei 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 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. Il trattamento del rischio di sicurezza è volto ad applicare una serie di misure di sicurezza che risultino in un equilibrio soddisfacente tra le esigenze degli utenti, i costi e il rischio di sicurezza residuo.

7. I requisiti, la portata e il grado di dettaglio specifici determinati dalla 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 garantire un adeguato livello di garanzie di sicurezza e accertare 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. L'SGC e gli Stati membri collaborano 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 dall'SGC e dagli Stati membri, 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 dei 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; e

e) *il ripristino:* misure di sicurezza volte a ripristinare il funzionamento in sicurezza del CIS.

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

17. Le autorità competenti 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 essenziali 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;

b) il potenziale danno ad altri che può derivare dall'interconnettività e dall'interdipendenza; e

c) la responsabilità personale, e l'obbligo di rendere conto, nella 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 dalla CAA nazionale di uno Stato membro.

26. Prima di essere raccomandati per approvazione del Consiglio o del segretario generale, conformemente all'articolo 10, paragrafo 6, 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 prevista per le ICUE che tali prodotti devono proteggere. Il Consiglio approva una politica di sicurezza sulla valutazione e l'approvazione di prodotto crittografici.

27. Ove giustificato da specifici motivi operativi, il Consiglio o il segretario generale, secondo i casi, può su raccomandazione del Comitato per la sicurezza dispensare dai requisiti di cui ai punti 25 o 26 e rilasciare un'approvazione temporanea per un determinato periodo conformemente alla procedura di cui all'articolo 10, paragrafo 6.

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. Il Consiglio 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; e

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'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 10, 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 competente.

37. I supporti informatici sono riutilizzati, declassati o declassificati secondo la politica di sicurezza da stabilire a norma dell'articolo 6, paragrafo 1.

Situazioni di emergenza

38. In deroga alle disposizioni della presente decisione, le procedure specifiche descritte di seguito possono essere applicate 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 38 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 38, è presentato un successivo rapporto all'autorità competente e al Comitato per la sicurezza.

III. FUNZIONI E AUTORITÀ DI GARANZIA DI SICUREZZA DELLE INFORMAZIONI

42. Negli Stati membri e presso l'SGC sono stabilite 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

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 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

45. L'autorità di approvazione degli apparati crittografici (CAA) ha il compito di assicurare che i prodotti crittografici siano conformi alla politica nazionale o alla politica del Consiglio in materia di crittografia. Essa concede l'approvazione di un prodotto crittografico per la protezione delle ICUE a un determinato livello di classifica nel suo contesto operativo. Per quanto riguarda gli Stati membri, la CAA è inoltre responsabile della valutazione dei prodotti crittografici.

Autorità di distribuzione degli apparati crittografici

46. L'autorità di distribuzione degli apparati crittografici (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

47. L'autorità di accreditamento di sicurezza (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 Consiglio 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 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 dell'SGC è responsabile dell'accreditamento di tutti i CIS operanti nell'ambito di competenza dell'SGC.

49. La SAA competente di uno Stato membro è responsabile dell'accreditamento dei CIS e delle relative componenti operanti nell'ambito di competenza di uno Stato membro.

50. Un comitato di accreditamento di sicurezza (SAB) comune è responsabile dell'accreditamento dei CIS nell'ambito di competenza sia della SAA dell'SGC che delle SAA degli Stati membri. Esso è composto di un rappresentante SAA per ciascuno Stato membro e vi partecipa un rappresentante SAA 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 dell'SGC. 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 e gli notifica tutte le dichiarazioni di accreditamento.

Autorità operativa per la garanzia di sicurezza delle informazioni

51. 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 gli SSRS, compresi la dichiarazione sul rischio residuo, le 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 di sicurezza e dispositivi 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 SecOps 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) svolgere analisi, esami e verifiche di sicurezza, 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 V

SICUREZZA INDUSTRIALE

I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 11. Esso stabilisce le 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 dall'SGC.

2. Il Consiglio approva una politica sulla sicurezza industriale che delinea in particolare requisiti dettagliati in ordine agli 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, l'SGC 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 l'SGC 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 la SCG, l'SGC tiene conto di tutti gli aspetti di sicurezza, tra cui la classifica di sicurezza assegnata all'informazione fornita e approvata che l'originatore dell'informazione deve usare per il contratto;

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, l'SGC 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 del contratto o subcontratto.

6. La SAL contiene le 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. L'NSA/DSA o altra autorità di sicurezza competente di uno Stato membro concede un FSC per indicare, secondo le disposizioni legislative e regolamentari 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. Il nulla osta è presentato all'SGC in quanto autorità contraente prima che al contraente o al subcontraente, effettivo o potenziale, possano essere comunicate delle ICUE o possa essere concesso un accesso alle ICUE.

9. Quando rilascia un FSC l'NSA/DSA competente, come minimo:

a) valuta l'integrità del soggetto industriale o di altra natura;

b) valuta la titolarità, il controllo o il potenziale di influenza indebita che può essere considerato un rischio per la sicurezza;

c) verifica che il soggetto industriale o di altra natura abbia stabilito un sistema di sicurezza nella struttura che contempli tutte le misure appropriate in materia di sicurezza necessarie per la protezione delle informazioni o del materiale classificato CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET conformemente ai requisiti stabiliti dalla presente decisione;

d) verifica che lo status in materia di sicurezza del personale della direzione, dei proprietari e degli impiegati che devono avere accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sia stato stabilito conformemente ai requisiti stabiliti dalla presente decisione;

e) verifica che il soggetto industriale o di altra natura abbia nominato un responsabile della sicurezza delle imprese che risponde alla direzione dell'osservanza degli obblighi di sicurezza all'interno del soggetto stesso.

10. Ove opportuno, l'SGC 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.

11. L'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.

12. L'NSA/DSA o altra autorità di sicurezza competente che ha rilasciato un FSC comunica all'SGC in quanto autorità contraente le modifiche inerenti l'FSC. In caso di subcontratto, l'NSA/DSA o altra autorità di sicurezza competente è informata di conseguenza.

13. La revoca dell'FSC da parte dell'NSA/DSA interessata o da altra autorità di sicurezza competente è motivo sufficiente per far sì che l'SGC in quanto autorità contraente estingua il contratto classificato o escluda l'offerente dalla gara.

IV. CONTRATTI O SUBCONTRATTI CLASSIFICATI

14. 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 entro un periodo di tempo determinato.

15. Una volta aggiudicato il contratto o il subcontratto classificato, l'SGC in quanto autorità contraente notifica all'NSA/DSA o altra autorità di sicurezza competente del contraente o subcontraente le disposizioni di sicurezza del contratto.

16. In caso di estinzione dei suddetti contratti l'SGC 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.

17. Di norma, alla cessazione del contratto o del subcontratto il contraente o subcontraente è tenuto a restituire all'autorità contraente le ICUE in suo possesso.

18. La SAL contiene disposizioni specifiche per l'eliminazione delle ICUE durante l'esecuzione o alla cessazione del contratto.

19. Se è autorizzato a conservare le ICUE alla cessazione del contratto il contraente o subcontraente continua a rispettare le norme minime comuni previste dalla presente decisione nonché a proteggere la riservatezza delle ICUE.

20. Le condizioni alle quali è ammesso il subcontratto da parte del contraente sono definite nel bando di gara e nel contratto.

21. Prima di subappaltare parti di un contratto classificato il contraente ottiene il consenso dell'SGC 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.

22. Spetta al contraente assicurare che tutte le attività del subcontratto si svolgano secondo le norme minime previste dalla presente decisione e di astenersi dal fornire ICUE al subcontraente senza previo consenso scritto dell'autorità contraente.

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

V. VISITE RELATIVE A CONTRATTI CLASSIFICATI

24. Se l'SGC, 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. Tuttavia, nel contesto di progetti specifici, le NSA/DSA possono anche convenire una procedura in base alla quale tali visite possono essere fissate direttamente.

25. Tutti i visitatori dispongono di un PSC adatto e di una necessità di conoscere per accedere alle ICUE relative ad un contratto dell'SGC.

26. I visitatori possono accedere solo alle ICUE relative all'oggetto della visita.

VI. TRASMISSIONE E TRASPORTO DI ICUE

27. Per la trasmissione elettronica di ICUE si applicano le pertinenti disposizioni dell'articolo 10 e dell'allegato IV.

28. In ordine al trasporto di ICUE, si applicano le pertinenti disposizioni dell'allegato III, conformemente alle disposizioni legislative e regolamentari nazionali.

29. 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 stato ottenuto dalle società addette al trasporto. In tal caso, il personale addetto alla spedizione dispone di un nulla osta di sicurezza conformemente all'allegato 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 dalle NSA/DSA o altra autorità di sicurezza competente interessata;

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 dall'NSA/DSA o da altra autorità di sicurezza competente degli Stati di spedizione e di destinazione.

VII. TRASMISSIONE DI ICUE A CONTRAENTI SITUATI IN PAESI TERZI

30. LE ICUE sono trasmesse a contraenti e subcontraenti situati in paesi terzi secondo misure di sicurezza convenute tra l'SGC in quanto autorità contraente e l'NSA/DSA del paese terzo interessato in cui il contraente ha sede.

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

31. Di concerto con l'NSA/DSA dello Stato membro, se opportuno, l'SGC 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.

32. 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 dall'SGC in quanto autorità contraente dei contratti o subcontratti contenenti informazioni classificate RESTREINT UE/EU RESTRICTED.

33. Per i contratti stipulati dall'SGC contenenti informazioni classificate RESTREINT UE/EU RESTRICTED, i contraenti o subcontraenti e relativo personale non sono tenuti a possedere un FSC o un PSC.

34. L'SGC 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.

35. Le condizioni alle quali è ammesso il subcontratto da parte del contraente sono conformi al punto 21.

36. Se un contratto comporta il trattamento di informazioni classificate RESTREINT UE/EU RESTRICTED in un CIS gestito da un contraente, l'SGC in qualità di 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 VI

SCAMBIO DI INFORMAZIONI CLASSIFICATE CON STATI TERZI E ORGANIZZAZIONI INTERNAZIONALI

I. INTRODUZIONE

1. Il presente allegato prevede le disposizioni di attuazione dell'articolo 12.

II. QUADRI CHE DISCIPLINANO LO SCAMBIO DI INFORMAZIONI CLASSIFICATE

2. Qualora il Consiglio ravvisi la necessità a lungo termine di scambiare informazioni classificate,

— è concluso un accordo sulla sicurezza delle informazioni, o

— sono pattuite intese amministrative,

in conformità dell'articolo 12, paragrafo 2 e delle sezioni III e IV e in base a una raccomandazione del Comitato per la sicurezza.

3. Qualora le ICUE prodotte ai fini di un'operazione PSDC debbano essere fornite a Stati terzi od organizzazioni internazionali che partecipano a detta operazione, e qualora non esista alcuno dei quadri normativi di cui al punto 2, lo scambio di ICUE con lo Stato terzo o l'organizzazione internazionale contributori è regolato, conformemente alla sezione V, a norma di:

— un accordo quadro di partecipazione, o

— un accordo di partecipazione ad hoc, o

— in assenza di uno degli accordi summenzionati, un'intesa amministrativa ad hoc.

4. In assenza di uno dei quadri di cui ai punti 2 e 3, e qualora sia adottata una decisione per comunicare ICUE a uno Stato terzo od organizzazione internazionale su una base eccezionale ad hoc conformemente alla sezione VI, sono richieste assicurazioni scritte dello Stato terzo od organizzazione internazionale in questione per garantire che questi proteggano qualsiasi ICUE comunicata conformemente ai principi fondamentali e alle norme minime stabiliti nella presente decisione.

III. ACCORDI SULLA SICUREZZA DELLE INFORMAZIONI

5. Gli accordi sulla sicurezza delle informazioni stabiliscono i principi fondamentali e le norme minime che disciplinano lo scambio di informazioni classificate tra l'UE e uno Stato terzo od organizzazione internazionale.

6. Gli accordi sulla sicurezza delle informazioni prevedono modalità tecniche di attuazione da concordare tra il Servizio di sicurezza dell'SGC, la DSCE e la competente autorità di sicurezza dello Stato terzo o dell'organizzazione internazionale in questione. Tali modalità tengono conto del livello di protezione garantito dalle normative, dalle strutture e dalle procedure in materia di sicurezza esistenti nello Stato terzo o nell'organizzazione internazionale in questione. Esse sono approvate dal Comitato per la sicurezza.

7. Le ICUE non sono oggetto di scambio per via elettronica, a meno che non sia esplicitamente previsto dall'accordo sulla sicurezza delle informazioni o dalle modalità tecniche di attuazione.

8. Gli accordi sulla sicurezza delle informazioni prevedono che prima dello scambio di informazioni classificate nel quadro dell'accordo il Servizio di sicurezza dell'SGC e la DSCE confermino che il destinatario è in grado di proteggere e salvaguardare le informazioni che gli vengono fornite in modo appropriato.

9. Quando il Consiglio conclude un accordo sulla sicurezza delle informazioni, ciascuna delle parti designa un ufficio di registrazione come principale punto d'ingresso e uscita per gli scambi delle informazioni classificate.

10. Per valutare l'efficacia delle normative, delle strutture e delle procedure in materia di sicurezza nello Stato terzo o nell'organizzazione internazionale in questione, il Servizio di sicurezza dell'SGC insieme con la DSCE e di comune accordo con detto Stato terzo od organizzazione internazionale conduce visite di valutazione. Tali visite di valutazione sono condotte conformemente alle pertinenti disposizioni dell'allegato III e valutano:

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

b) eventuali aspetti specifici della politica di sicurezza e del modo in cui è organizzata la sicurezza nello Stato terzo o nell'organizzazione internazionale che potrebbero avere un impatto sul livello delle informazioni classificate che possono essere oggetto di scambio;

c) le misure e le procedure di sicurezza effettivamente attuate; e

d) le procedure per il nulla osta di sicurezza per il livello delle ICUE da comunicare.

11. La squadra che conduce una visita di valutazione a nome dell'UE valuta se le norme e procedure di sicurezza nello Stato terzo o nell'organizzazione internazionale in questione sono adeguate alla protezione delle ICUE di un determinato livello.

12. I risultati di tali visite sono illustrati in una relazione sulla cui base il Comitato per la sicurezza stabilisce il livello massimo delle ICUE che possono essere scambiate in forma cartacea e, in caso, con mezzi elettronici con il terzo in questione nonché eventuali condizioni specifiche applicabili a tale scambio.

13. Viene compiuto ogni sforzo per effettuare una visita completa di valutazione della sicurezza nello Stato terzo o nell'organizzazione internazionale in questione prima che il Comitato per la sicurezza approvi le modalità di attuazione al fine di accertare la natura e l'efficienza del sistema di sicurezza esistente. Tuttavia, ove ciò non sia possibile, il Comitato per la sicurezza riceve una relazione quanto più completa possibile dal Servizio di sicurezza dell'SGC, in base alle informazioni in suo possesso, in cui viene informato delle norme di sicurezza applicabili e del modo in cui è organizzata la sicurezza nello Stato terzo o nell'organizzazione internazionale in questione.

14. Il Comitato per la sicurezza può decidere che, in attesa dell'esame del risultato di una visita di valutazione, non si possano comunicare ICUE o le si possano comunicare solo fino a un determinato livello, oppure può stabilire altre condizioni specifiche applicabili alla comunicazione delle ICUE allo Stato terzo o all'organizzazione internazionale in questione. Ciò viene notificato dal Servizio di sicurezza dell'SGC allo Stato terzo o all'organizzazione internazionale in questione.

15. Di comune accordo con lo Stato terzo o l'organizzazione internazionale in questione, il Servizio di sicurezza dell'SGC effettua, a intervalli regolari, visite di valutazione di follow up al fine di verificare che le intese continuino a soddisfare le norme minime concordate.

16. Quando l'accordo sulla sicurezza delle informazioni è in vigore e le informazioni classificate sono scambiate con lo Stato terzo o l'organizzazione internazionale in questione, il Comitato per la sicurezza può decidere di modificare il livello massimo delle ICUE che possono essere scambiate in forma cartacea o con mezzi elettronici, in particolare alla luce di eventuali visite di valutazione di follow up.

IV. INTESE AMMINISTRATIVE

17. Qualora sussista una necessità a lungo termine di scambiare informazioni classificate in generale di livello non superiore a RESTREINT UE/EU RESTRICTED con uno Stato terzo o un'organizzazione internazionale e qualora il Comitato per la Sicurezza abbia stabilito che il terzo in questione non possiede un sistema di sicurezza sufficientemente sviluppato da consentirgli di concludere un accordo sulla sicurezza delle informazioni, il segretario generale, previa approvazione del Consiglio, può pattuire intese amministrative con le autorità competenti dello Stato terzo o dell'organizzazione internazionale in questione.

18. Qualora si debba istituire rapidamente, per ragioni operative urgenti, un quadro normativo per lo scambio di informazioni classificate, eccezionalmente il Consiglio può decidere di pattuire intese amministrative per lo scambio di informazioni di un livello di classifica più elevato.

19. Le intese amministrative assumono di norma la forma di uno scambio di lettere.

20. Prima che le ICUE siano effettivamente comunicate allo Stato terzo o all'organizzazione internazionale in questione si effettua la visita di valutazione di cui al punto 10 e si trasmette la relativa relazione al Comitato per la sicurezza che la deve giudicare soddisfacente. Tuttavia, qualora siano sottoposte all'esame del Consiglio ragioni eccezionali per uno scambio urgente di informazioni classificate, possono essere comunicate ICUE purché venga compiuto ogni sforzo per effettuare tale visita di valutazione il più presto possibile.

21. Le ICUE non sono oggetto di scambio per via elettronica a meno che non sia esplicitamente previsto dall'intesa amministrativa.

V. SCAMBIO DI INFORMAZIONI CLASSIFICATE NEL CONTESTO DI OPERAZIONI PSDC

22. Gli accordi quadro di partecipazione disciplinano la partecipazione di Stati terzi od organizzazioni internazionali alle operazioni PSDC. Tali accordi includono disposizioni sulla comunicazione di ICUE prodotte ai fini delle operazioni PSDC agli Stati terzi o alle organizzazioni internazionali contributori. Il livello massimo di classifica delle ICUE che possono essere scambiate è RESTREINT UE/EU RESTRICTED per operazioni civili PSDC e CONFIDENTIEL UE/EU CONFIDENTIAL per operazioni militari PSDC, salvo se diversamente stabilito nella decisione che istituisce ciascuna operazione PSDC.

23. Gli accordi di partecipazione ad hoc conclusi per una specifica operazione PSDC includono disposizioni sulla comunicazione di ICUE prodotte ai fini di detta operazione allo Stato terzo o all'organizzazione internazionale contributori. Il livello massimo di classifica delle ICUE che possono essere scambiate è RESTREINT UE/EU RESTRICTED per operazioni civili PSDC e CONFIDENTIEL UE/EU CONFIDENTIAL per operazioni militari PSDC, salvo se diversamente stabilito nell'azione comune che istituisce ciascuna operazione PSDC.

24. Le intese amministrative ad hoc relative alla partecipazione di uno Stato terzo o di un'organizzazione internazionale a un'operazione specifica PSDC possono contemplare tra l'altro la comunicazione di ICUE prodotte ai fini dell'operazione a tale Stato terzo od organizzazione internazionale. Tali intese amministrative ad hoc sono pattuite conformemente alle procedure di cui ai punti 17 e 18 della sezione IV. Il livello massimo di classifica delle ICUE che possono essere scambiate è RESTREINT UE/EU RESTRICTED per operazioni civili PSDC e CONFIDENTIEL UE/EU CONFIDENTIAL per operazioni militari PSDC, salvo se diversamente stabilito nella decisione che istituisce ciascuna operazione PSDC.

25. Non sono richieste modalità di attuazione o visite di valutazione prima di attuare le disposizioni sulla comunicazione di ICUE nel contesto dei punti 22, 23 e 24.

26. Qualora lo Stato ospitante nel cui territorio si svolge un'operazione PSDC non abbia concluso un accordo sulla sicurezza delle informazioni o pattuito intese amministrative con l'UE per lo scambio di informazioni classificate, nel caso di una necessità operativa specifica e immediata può essere adottata un'intesa amministrativa ad hoc. Questa possibilità è prevista nella decisione che istituisce l'operazione PSDC. Le ICUE comunicate in tali circostanze sono limitate a quelle prodotte ai fini dell'operazione PSDC e classificate di livello non superiore a RESTREINT UE/EU RESTRICTED. A norma di tale intesa amministrativa ad hoc lo Stato ospitante si impegna a proteggere le ICUE conformemente a norme minime che non sono meno rigorose di quelle previste nella presente decisione.

27. Le disposizioni in materia di informazioni classificate da includere negli accordi quadro di partecipazione, negli accordi di partecipazione ad hoc e nelle intese amministrative ad hoc di cui ai punti da 22 a 24 prevedono che lo Stato terzo o l'organizzazione internazionale in questione garantiscano che il personale distaccato per partecipare a qualsiasi operazione proteggerà le ICUE conformemente alle norme di sicurezza del Consiglio e agli ulteriori orientamenti emanati dalle autorità competenti, tra cui la catena di comando dell'operazione.

28. Se un accordo sulla sicurezza delle informazioni è successivamente concluso tra l'UE e uno Stato terzo o un'organizzazione internazionale contributori, l'accordo sulla sicurezza delle informazioni prevale su qualsiasi accordo quadro di partecipazione, accordo di partecipazione ad hoc o intesa amministrativa ad hoc per quanto riguarda lo scambio e il trattamento delle ICUE.

29. Nell'ambito di un accordo quadro di partecipazione, di un accordo di partecipazione ad hoc o di un'intesa amministrativa ad hoc conclusi con uno Stato terzo o un'organizzazione internazionale non sono permessi scambi di ICUE per via elettronica, a meno che non siano esplicitamente previsti nell'accordo o nell'intesa in questione.

30. Le ICUE prodotte ai fini di un'operazione PSDC possono essere diffuse al personale distaccato da Stati terzi o da organizzazioni internazionali per partecipare a detta operazione conformemente ai punti da 22 a 29. Al momento di autorizzare l'accesso alle ICUE nei locali o nei CIS di un'operazione PSDC da parte di tale personale, sono applicate misure (tra cui la registrazione delle ICUE diffuse) per attenuare il rischio di perdita o di compromissione. Tali misure sono definite nei documenti di pianificazione o di missione pertinenti.

VI. COMUNICAZIONE ECCEZIONALE AD HOC DI ICUE

31. Qualora non sia istituito alcun quadro normativo conformemente alle sezioni III, IV e V e qualora il Consiglio o uno dei suoi organi preparatori ravvisi la necessità eccezionale di comunicare ICUE a uno Stato terzo o un'organizzazione internazionale, l'SGC:

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, sulla base delle informazioni disponibili, ad emettere una raccomandazione concernente la fiducia che può essere accordata nelle normative, strutture e procedure in materia di sicurezza dello Stato terzo o dell'organizzazione internazionale cui devono essere comunicate le ICUE.

32. Se il Comitato per la sicurezza emette una raccomandazione favorevole alla comunicazione delle ICUE, la questione è sottoposta al Comitato dei Rappresentanti Permanenti (Coreper), che adotta una decisione in merito a detta comunicazione.

33. Se la raccomandazione del Comitato per la sicurezza non è favorevole alla comunicazione delle ICUE:

a) per questioni relative alla PESC/PSDC, il Comitato politico e di sicurezza discute la questione e formula una raccomandazione di decisione del Coreper;

b) per tutte le altre questioni, il Coreper discute al riguardo e adotta una decisione.

34. Ove lo si ritenga opportuno e fatto salvo il consenso preliminare scritto dell'originatore, il Coreper può decidere che le informazioni classificate possano essere comunicate solo in parte o solo se declassate o declassificate in via preliminare, o che le informazioni da comunicare siano messe a punto senza riferimento alla fonte o al livello originario di classifica UE.

35. A seguito di una decisione di comunicare ICUE, l'SGC trasmette il documento in questione recante un contrassegno di divulgabilità che indica lo Stato terzo o l'organizzazione internazionale a cui è stato comunicato. Prima o al momento della comunicazione effettiva, il terzo in questione si impegna per iscritto a proteggere le ICUE che riceve conformemente ai principi fondamentali e alle norme minime stabiliti nella presente decisione.

VII. FACOLTÀ DI COMUNICARE ICUE A STATI TERZI OD ORGANIZZAZIONI INTERNAZIONALI

36. Qualora esista un quadro normativo in conformità al punto 2 per lo scambio di informazioni classificate con uno Stato terzo o un'organizzazione internazionale, il Consiglio adotta la decisione di autorizzare il segretario generale a comunicare le ICUE allo Stato terzo o all'organizzazione internazionale in questione, conformemente al principio del consenso dell'originatore.

37. Qualora esista un quadro normativo in conformità al punto 3 per lo scambio di informazioni classificate con uno Stato terzo o un'organizzazione internazionale, il segretario generale è autorizzato a comunicare le ICUE conformemente alla decisione che istituisce l'operazione PSDC e al principio del consenso dell'originatore.

38. Il segretario generale può delegare tale facoltà ad alti funzionari dell'SGC o altre persone poste sotto la sua autorità.

Appendici

Appendice A

DEFINIZIONI

Ai fini della presente decisione si intende per:

«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), un'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;

«certificato di nulla osta di sicurezza personale» (PSCC), un certificato rilasciato da un'autorità competente attestante che una persona è in possesso del nulla osta di sicurezza e possiede un PSC nazionale o un PSC UE in corso di validità, in cui figura il livello di ICUE cui detta persona può accedere (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), 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;

«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 l'SGC 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;

«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» cfr. l'articolo 10, paragrafo 1;

«gestione delle informazioni classificate» cfr. l'articolo 9, paragrafo 1;

«guida alle classifiche di sicurezza» (SCG), un 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; se esistente l'SCG fa parte della SAL;

«indagine di sicurezza» le procedure investigative condotte dall'autorità competente di uno Stato membro conformemente alle sue disposizioni legislative e regolamentari nazionali volte ad ottenere la garanzia dell'inesistenza di informazioni negative note sul conto di una persona che osterebbero alla concessione di un PSC nazionale o di un PSC UE per accedere alle ICUE fino a un livello specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore);

«informazioni classificate UE» (ICUE) — cfr. l'articolo 2, paragrafo 1;

«interconnessione» — cfr. l'allegato 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), un pacchetto di condizioni contrattuali specifiche emesso dall'autorità contraente, che è parte integrante di ogni contratto classificato implicante l'accesso o la creazione di ICUE, in cui sono individuati i requisiti di sicurezza o gli elementi del contratto che richiedono una protezione di sicurezza;

«materiale» qualsiasi documento od elemento di macchinario o attrezzatura, sia sotto forma di prodotto finito sia in corso di lavorazione;

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

«minaccia» una causa potenziale di un incidente indesiderato che può recar danno a un'organizzazione o a qualsiasi sistema in uso; tali minacce possono essere accidentali o intenzionali (dolose) e sono caratterizzate da elementi di minaccia, potenziali obiettivi e metodologie d'attacco;

«modo di funzionamento in condizioni di sicurezza», la definizione delle condizioni in cui funziona un CIS in base alla classifica delle informazioni trattate e ai livelli di nulla osta personale, alle approvazioni dell'accesso formale e alla necessità di conoscere dei suoi utenti. Esistono quattro modi di funzionamento per trattare o trasmettere informazioni classificate: modo esclusivo, modo predominante, modo compartimentato e modo multilivello; si intende per:

— «modo esclusivo» un modo di funzionamento in cui tutte le persone che hanno accesso al CIS sono in possesso di un nulla osta per il livello più elevato di classifica delle informazioni trattate all'interno del CIS e con la comune necessità di conoscere rispetto a tutte le informazioni trattate all'interno del CIS,

— «modo predominante» un modo di funzionamento in cui tutte le persone che hanno accesso al CIS sono in possesso di un nulla osta per il livello più elevato di classifica delle informazioni trattate all'interno del CIS, ma non tutte le persone che hanno accesso al CIS hanno una comune necessità di conoscere rispetto alle informazioni trattate all'interno del CIS; l'autorizzazione di accesso alle informazioni può essere concessa da una persona,

— «modo compartimentato», un modo di funzionamento in cui tutte le persone che hanno accesso al CIS sono in possesso di un nulla osta per il livello più elevato di classifica delle informazioni trattate all'interno del CIS, ma non tutte le persone che hanno accesso al CIS hanno un'autorizzazione formale per accedere a tutte le informazioni trattate all'interno del CIS; l'autorizzazione formale implica una gestione centrale formale di controllo dell'accesso distinta dalla discrezionalità di una persona di consentire l'accesso,

— «modo multilivello», un modo di funzionamento in cui non tutte le persone che hanno accesso al CIS sono in possesso di un nulla osta per il livello più elevato di classifica delle informazioni trattate all'interno del CIS e non tutte le persone che hanno accesso al CIS hanno una comune necessità di conoscere rispetto alle informazioni trattate all'interno del CIS,

«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), uno o entrambi dei seguenti nulla osta:

— «nulla osta di sicurezza personale UE» (PSC UE) per l'accesso alle ICUE: un'autorizzazione dell'autorità dell'SGC che ha il potere di nomina adottata conformemente alla presente decisione 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»,

— «nulla osta di sicurezza personale nazionale» (PSC nazionale) per l'accesso alle ICUE: una dichiarazione dell'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 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»;

«operazione PSDC» un'operazione di gestione militare o civile delle crisi stabilita 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 di sicurezza» l'intera procedura che consiste nell'individuare, controllare e ridurre al minimo eventi incerti che possono incidere sulla sicurezza di un'organizzazione o di un qualsiasi sistema in uso. Essa comprende tutte le attività correlate al rischio, tra cui la valutazione, il trattamento, l'accettazione e la comunicazione;

«registrazione» cfr. l'allegato III, punto 18;

«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 e ai suoi beni materiali o immateriali. È calcolato come una combinazione tra le probabilità del verificarsi delle minacce e il loro impatto:

— l'«accettazione del rischio» costituisce la decisione di accettare la permanenza di un rischio residuo in seguito al trattamento del rischio,

— la «valutazione del rischio» consiste nell'identificare le minacce e le vulnerabilità e nell'effettuare le relative analisi del rischio, ossia l'analisi della probabilità e dell'impatto,

— la «comunicazione del rischio» consiste nello sviluppare 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,

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

«rischio residuo» il rischio che resta una volta attuate delle 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» cfr. l'articolo 7, paragrafo 1;

«sicurezza industriale» cfr. l'articolo 11, paragrafo 1;

«sicurezza materiale» cfr. l'articolo 8, paragrafo 1;

«sistema di comunicazione e informazione» (CIS) — cfr. l'articolo 10, paragrafo 2;

«soggetto industriale o di altra natura», un soggetto che si occupa della fornitura di beni, della realizzazione di opere 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 realizzazione di opere o di prestazione di servizi, stipulato fra un contraente dell'SGC 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, tutte le azioni 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 la loro raccolta, visualizzazione, trasmissione e conservazione;

«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.

Appendice B

EQUIVALENZA DELLE CLASSIFICHE DI SICUREZZA

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONDIFENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgio	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Nota [1] infra
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Repubblica ceca	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danimarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	STRENG GEHEIM	GEHEIM	VS [2] — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abbr: ΑΑΠ	Απόρρητο Abbr: (ΑΠ)	Εμπιστευτικό Abbr: (ΕΜ)	Περιορισμένης Χρήσης Abbr: (ΠΧ)
Spagna	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francia	Très Secret Défense	Secret Défense	Confidentiel Défense	*nota [3] infra*
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Cipro	Άκρως Απόρρητο Abbr: (ΑΑΠ)	Απόρρητο Abbr: (ΑΠ)	Εμπιστευτικό Abbr: (ΕΜ)	Περιορισμένης Χρήσης Abbr: (ΠΧ)
Lettonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Lussemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungheria	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Għola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Paesi Bassi	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portogallo	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONDIFENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovacchia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Svezia ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Regno Unito	Top Secret	Secret	Confidential	Restricted

([1]) Diffusion Restreinte/Beperkte Verspreiding non è una classifica di sicurezza in Belgio. Il Belgio tratta e protegge le informazioni «RESTREINT UE/EU RESTRICTED» in modo non meno rigoroso delle norme e procedure descritte nella normativa di sicurezza del Consiglio dell'Unione europea.

([2]) Germania: VS = Verschlusssache (informazioni classificate).

([3]) La Francia non usa il grado di classifica «RESTREINT» nel suo sistema nazionale. La Francia tratta e protegge le informazioni «RESTREINT UE/EU RESTRICTED» in modo non meno rigoroso delle norme e procedure descritte nella normativa di sicurezza del Consiglio dell'Unione europea.

([4]) Per la Svezia: i contrassegni di classifica di sicurezza della riga superiore sono usati dalle autorità della difesa e i contrassegni della riga inferiore sono usati dalle altre autorità.

Appendice C

ELENCO DELLE AUTORITÀ NAZIONALI DI SICUREZZA (NSA)

BELGIO
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. segretariato: + 32 25014542
Fax + 32 25014596
E-mail: nvo-ans@diplobel.fed.be

DANIMARCA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel. + 45 33148888
Fax + 45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel. + 45 33325566
Fax + 45 33931320

BULGARIA
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel. + 359 29215911
Fax + 359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

GERMANIA
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101
11014 Berlin

Tel. + 49 30186810
Fax + 49 3018681-1441
E-mail: oesIII3@bmi.bund.de

REPUBBLICA CECA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel. + 420 257283335
Fax + 420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

ESTONIA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel. +372 7170113-117
Fax +372 7170213
E-mail: nsa@kmin.ee

IRLANDA
National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2 IRELAND

Tel. + 353 14780822
Fax + 353 14082959

SPAGNA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel. + 34 913725000
Fax + 34 913725808
E-mail: nsa-sp@areatec.com

GRECIA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 — Χολαργός
(Αθήνα)

Tel. + 30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Fax + 30 2106536279
+ 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens

Tel. + 30 2106572045
+ 30 2106572009
Fax + 30 2106536279
+ 30 2106577612

FRANCIA
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel. + 33 171758177
Fax + 33 171758200

ITALIA
Presidenza del Consiglio dei Ministri
Autorità nazionale per la sicurezza
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma RM

Tel. + 39 0661174266
Fax + 39 064885273

CIPRO
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Tel. + 357 22807569-7643-7764
Fax + 357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tel. + 357 22807569-7643-7764
Fax + 357 22302351
E-mail: cynsa@mod.gov.cy

LUSSEMBURGO
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tel. + 352 24782210 central
+ 352 24782253 direct
Fax + 352 24782243

UNGHERIA
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tel. + 36 13469652
Fax + 36 13469658
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
Valletta

Tel. + 356 21249844
Fax + 356 25695321

LETTONIA
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
Riga, LV-1001

Tel. +371 67025418
Fax +371 67025454
Email: ndi@sab.gov.lv

LITUANIA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Tel.+ 370 52663201-2
Fax + 370 52663200
E-mail: nsa@vsd.lt

PAESI BASSI
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel. + 31 703204400
Fax + 31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel. + 31 703187060
Fax + 31 703187522

AUSTRIA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tel. + 43 1531152594
Fax + 43 1531152615
E-mail: ISK@bka.gv.at

POLONIA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa

Tel. + 48 225857360
Fax + 48 225858509
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Buremu
Oczki 1
02-007 Warszawa

Tel. + 48 226841247
Fax + 48 226841076
E-mail: skw@skw.gov.pl

ROMANIA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest

Tel. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

PORTOGALLO
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel. +351 213031710
Fax +351 213031711

SLOVENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana

Tel. + 386 14781390
Fax + 386 14781399

SLOVACCHIA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel. + 421 268692314
Fax + 421 263824005
Website: www.nbusr.sk

SVEZIA
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm

Tel. + 46 84051000
Fax + 46 87231176
E-mail: ud-nsa@foreign.ministry.se

FINLANDIA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Tel. + 358 916056487-4
Fax + 358 916055140
E-mail: NSA@formin.fi

REGNO UNITO
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Tel. + 44 2072765649-5497
Fax + 44 2072765651
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendice D

ELENCO DELLE ABBREVIAZIONI

Abbreviazione	Significato
AQUA	Appropriately Qualified Authority — Autorità di validazione qualificata
BPS	Boundary Protection Services — Servizi di protezione perimetrale
CAA	Crypto Approval Authority — Autorità di approvazione degli apparati crittografici
CCTV	Closed Circuit Television — Televisione a circuito chiuso
CDA	Crypto Distribution Authority — Autorità di distribuzione degli apparati crittografici
CIS	Communication and Information Systems handling EUCI — Sistemi di comunicazione e informazione che trattano ICUE
COREPER	Comitato dei Rappresentanti Permanenti
DSA	Designated Security Authority — Autorità di sicurezza designata
DSCE	Direzione della sicurezza della Commissione europea
FSC	Facility Security Clearance — Nulla osta di sicurezza delle imprese
IA	Information Assurance — Garanzia di sicurezza delle informazioni
IAA	Information Assurance Authority — Autorità la garanzia di sicurezza delle informazioni
ICUE	Informazioni classificate UE
IDS	Intrusion Detection System — Sistema di rilevamento delle intrusioni
NSA	National Security Authority — Autorità di sicurezza nazionale
PESC	Politica estera e di sicurezza comune
PSDC	Politica di sicurezza e di difesa comune
PSC	Personnel Security Clearance — Nulla osta di sicurezza personale
PSCC	Personnel Security Clearance Certificate — Certificato di nulla osta di sicurezza personale
PSI	Programme/Project Security Instructions — Istruzioni di sicurezza del programma/progetto
RSUE	Rappresentante speciale dell'UE
SAA	Security Accreditation Authority — Autorità di accreditamento di sicurezza
SAB	Security Accreditation Board — Comitato di accreditamento di sicurezza
SAL	Security Aspects Letter — Lettera sugli aspetti di sicurezza
SecOP	Security Operating Procedures — Procedure operative di sicurezza
SCG	Security Classification Guide — Guida alle classifiche di sicurezza
SGC	Segretariato generale del Consiglio
SSRS	System-Specific Security Requirement Statement — Dichiarazione relativa ai requisiti di sicurezza specifici del sistema
TA	Tempest Authority — Autorità TEMPEST
TI	Tecnologia dell'informazione