COMMISSIONE
EUROPEA

Bruxelles, 22.3.2022
COM(2022) 119 final

2022/0084 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione

{SWD(2022) 65 final} - {SWD(2022) 66 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

La presente proposta fa parte della strategia dell'UE per l'Unione della sicurezza[1], adottata dalla Commissione il 24 luglio 2020, che enuncia l'impegno ad apportare il valore aggiunto dell'Unione europea agli sforzi nazionali nel settore della sicurezza. Questo impegno include l'iniziativa volta a razionalizzare i quadri giuridici interni per la sicurezza delle informazioni nell'insieme delle istituzioni e degli organi dell'Unione.

Un elemento fondamentale dell'agenda strategica per il periodo 2019-2024, adottata dal Consiglio europeo nel giugno 2019, è proteggere le nostre società dalle minacce in continua evoluzione che incombono sulle informazioni trattate dalle istituzioni e dagli organi dell'Unione. Nelle sue conclusioni[2] il Consiglio europeo ha invitato in particolare "le istituzioni dell'UE, insieme agli Stati membri, a lavorare a misure per aumentare la resilienza e migliorare la cultura della sicurezza dell'UE contro le minacce informatiche e ibride provenienti dall'esterno dell'UE, nonché per meglio proteggere da qualsiasi attività dolosa le reti di informazione e di comunicazione dell'UE e i suoi processi decisionali".

Analogamente, il Consiglio "Affari generali" del dicembre 2019[3] ha concluso che le istituzioni e gli organi dell'UE, con il sostegno degli Stati membri, dovrebbero elaborare e mettere in pratica un insieme completo di misure destinate a garantirne la sicurezza. Questa conclusione fa eco alla richiesta di lunga data del comitato per la sicurezza del Consiglio di elaborare un nucleo comune di norme di sicurezza per il Consiglio, la Commissione e il Servizio europeo per l'azione esterna[4].

Attualmente le istituzioni e gli organi dell'Unione hanno le proprie norme di sicurezza delle informazioni, basate sul proprio regolamento interno o atto istitutivo, oppure non ne hanno affatto. È il caso soprattutto di alcune piccole entità, che non dispongono di politiche formali in materia di sicurezza delle informazioni.

Considerati il numero sempre crescente di informazioni sensibili non classificate e di informazioni classificate UE ("ICUE") che le istituzioni e gli organi dell'Unione devono condividere tra loro e il drammatico sviluppo del panorama delle minacce, l'amministrazione europea è esposta ad attacchi in tutti i suoi settori di attività. Le informazioni trattate dalle nostre istituzioni e dai nostri organi sono molto interessanti per gli autori delle minacce e devono essere adeguatamente protette. Ciò richiede un'azione rapida per migliorarne la protezione.

Pertanto, al fine di aumentare la protezione delle informazioni trattate dall'amministrazione europea, la presente iniziativa mira a razionalizzare i diversi quadri giuridici delle istituzioni e degli organi dell'Unione in questo settore:

- stabilendo categorie armonizzate e complete di informazioni, nonché norme comuni in materia di trattamento per tutte le istituzioni e tutti gli organi dell'Unione;

---

1 Comunicazione sulla strategia dell'UE per l'Unione della sicurezza, COM(2020) 605 del 24 luglio 2020 (priorità strategica "Un ambiente di sicurezza adeguato alle esigenze del futuro").

2 EUCO 9/19.

3 14972/19.

4 WK 10563/2018 INIT sezione 9.

- istituendo un sistema snello di cooperazione in materia di sicurezza delle informazioni tra le istituzioni e gli organi dell'Unione, in grado di promuovere una cultura coerente della sicurezza delle informazioni in tutta l'amministrazione europea;
- modernizzando le politiche in materia di sicurezza delle informazioni a tutti i livelli di classifica/categorizzazione, per tutte le istituzioni e tutti gli organi dell'Unione, tenendo conto della trasformazione digitale e dello sviluppo del telelavoro come pratica strutturale.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

L'iniziativa è conforme a un'ampia gamma di politiche dell'UE nel settore della sicurezza e della sicurezza delle informazioni.

Nel 2016 il Parlamento europeo e il Consiglio hanno adottato una direttiva[5] recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Tale direttiva è stata la prima misura legislativa a livello dell'UE volta ad aumentare la cooperazione tra gli Stati membri in materia di cibersicurezza. Sebbene nel dicembre 2020 la Commissione abbia adottato una proposta di revisione di tale strumento, che introduce misure di vigilanza per le autorità nazionali, l'amministrazione dell'Unione rimane esclusa dal suo ambito di applicazione.

Nella stessa ottica e per integrare gli sforzi degli Stati membri nel settore della sicurezza, è di fondamentale importanza che le istituzioni e gli organi dell'Unione raggiungano un elevato livello di protezione delle loro informazioni e dei relativi sistemi di informazione e comunicazione al fine di salvaguardare la sicurezza delle informazioni.

Nel luglio 2020 la Commissione ha adottato la strategia per l'Unione della sicurezza[6], che comprende un impegno globale dell'UE a integrare gli sforzi degli Stati membri in tutti i settori della sicurezza. Tale strategia, che va dal 2020 al 2025, delinea quattro principali pilastri d'azione: assicurare un ambiente della sicurezza adeguato alle esigenze future, affrontare le minacce in evoluzione, proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata e costruire un forte ecosistema europeo della sicurezza. Molti dei temi affrontati nell'ambito di questi pilastri riguardano la sicurezza delle informazioni, la cibersicurezza, la cooperazione e lo scambio di informazioni e le infrastrutture critiche.

In linea con la strategia per l'Unione della sicurezza, la Commissione europea propone la creazione di un insieme minimo di norme in materia di sicurezza delle informazioni in tutte le istituzioni e tutti gli organi dell'Unione, che darà l'avvio a norme comuni rigorose e obbligatorie per lo scambio sicuro di informazioni. La presente iniziativa rappresenta l'impegno delle istituzioni e degli organi a fissare, in seno all'amministrazione europea, lo stesso livello di ambizione nel settore della sicurezza richiesto dagli Stati membri.

Il 16 dicembre 2020 la Commissione e l'alto rappresentante per gli affari esteri e la politica di sicurezza hanno presentato una nuova strategia dell'UE per la cibersicurezza[7], che definisce le priorità e le azioni chiave per rafforzare la resilienza, l'autonomia, la leadership e la capacità

---

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

6 C(2020) 605.

7 La strategia dell'UE in materia di cibersicurezza per il decennio digitale | Plasmare il futuro digitale dell'Europa (europa.eu), compresi una comunicazione congiunta con l'alto rappresentante per gli affari esteri e la politica di sicurezza (JOIN(2020)18) e una direttiva sulla sicurezza delle reti e dell'informazione (NIS) riveduta (COM(2020) 823).

operativa dell'Europa di fronte alle minacce crescenti e complesse per le sue reti e i suoi sistemi informativi, e per promuovere un ciberspazio globale e aperto e i relativi partenariati internazionali. È altrettanto importante che le istituzioni e gli organi dell'Unione contribuiscano al conseguimento di tali priorità stabilendo requisiti equivalenti sia nel settore della sicurezza delle informazioni che in quello della cibersicurezza.

La presente proposta, unitamente alla proposta di regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, mira a completare il quadro normativo della strategia per l'Unione della sicurezza con requisiti specifici per l'amministrazione europea. In considerazione delle interconnessioni esistenti tra la sicurezza delle informazioni e la cibersicurezza, è opportuno assicurare che queste due proposte seguano un approccio coerente alla protezione delle informazioni non classificate.

- **Coerenza con le altre normative dell'Unione**

La presente iniziativa tiene conto anche di altre normative dell'Unione pertinenti per la sicurezza delle informazioni.

Nel settore della protezione dei dati vige il regolamento (UE) 2018/1725[8] sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, applicabile all'amministrazione dell'Unione europea e della Comunità europea dell'energia atomica ("Euratom"). Nella stessa ottica, è necessario ricordare che per alcune istituzioni e alcuni organi dell'Unione i legislatori dell'UE hanno adottato norme specifiche pertinenti per la protezione dei dati personali.

Nel settore della trasparenza, la presente proposta si basa sui principi sanciti dal regolamento (CE) n. 1049/2001[9] relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione, per quanto riguarda altre norme pertinenti.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

Tenuto conto dell'obiettivo e del contenuto della presente proposta, la sua base giuridica più appropriata è l'articolo 298 del trattato sul funzionamento dell'Unione europea (TFUE) e l'articolo 106 bis del trattato che istituisce la Comunità europea dell'energia atomica.

L'articolo 298 TFUE è stato introdotto dal trattato di Lisbona e consente ai legislatori di stabilire disposizioni per creare un'amministrazione efficace e indipendente che assista le istituzioni, gli organi e gli organismi nell'assolvimento dei loro compiti.

Un'amministrazione efficace e indipendente ha bisogno che sia garantita la sicurezza delle sue informazioni. Al fine di svolgere i loro compiti, le istituzioni e gli organi dell'Unione devono disporre di un ambiente sicuro per le informazioni che trattano e conservano quotidianamente. Inoltre, fornire una base comune di norme obbligatorie per tutti garantirebbe un elevato livello di sicurezza, ridurrebbe il rischio di anelli deboli nel sostegno all'interoperabilità tra le

[8] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39)

[9] Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

istituzioni e gli organi e stimolerebbe le sinergie, rafforzando in tal modo la resilienza dell'amministrazione di fronte alle minacce in evoluzione.

Peraltro, perseguendo l'obiettivo generale di conseguire un elevato livello comune di sicurezza per le ICUE e le informazioni non classificate trattate e conservate dalle istituzioni e dagli organi dell'Unione, la presente proposta consente all'amministrazione europea di proteggersi meglio dalle interferenze esterne e dalle attività di spionaggio.

L'articolo 298 TFUE consente all'Unione di stabilire norme comuni per l'intera amministrazione europea al fine di garantire che tutte le istituzioni e tutti gli organi dell'Unione trattino le ICUE e le informazioni non classificate allo stesso modo. Il regolamento proposto stabilisce pertanto norme applicabili all'amministrazione e può indirettamente imporre obblighi solo alle persone che svolgono compiti per conto di tale amministrazione o su base contrattuale (esclusi i commissari, i rappresentanti degli Stati membri che agiscono in seno al Consiglio, i membri del Parlamento europeo, i giudici degli organi giurisdizionali dell'Unione o i membri della Corte dei conti europea).

Conformemente all'articolo 298 TFUE, il Parlamento europeo e il Consiglio deliberano mediante regolamento e secondo la procedura legislativa ordinaria.

La presente proposta necessita di una base giuridica supplementare in quanto copre anche le informazioni relative ad alcune attività della Comunità europea dell'energia atomica. Tali informazioni non sono informazioni classificate Euratom, ma sono trattate dalle istituzioni e dagli organi dell'Unione nell'ambito del regime generale delle ICUE.

Questa base giuridica supplementare è costituita dall'articolo 106 bis del trattato che istituisce la Comunità europea dell'energia atomica, che rende l'articolo 298 TFUE applicabile anche alle suddette attività dell'Euratom.

- **Sussidiarietà (per la competenza non esclusiva)**

In virtù del principio di sussidiarietà enunciato all'articolo 5, paragrafo 3, del trattato sull'Unione europea (TUE), l'Unione interviene soltanto se e in quanto gli obiettivi dell'azione prevista non possono essere conseguiti in misura sufficiente dagli Stati membri, ma possono, a motivo della portata o degli effetti delle azioni in questione, essere conseguiti meglio a livello di Unione.

Poiché solo l'Unione può adottare norme che disciplinano le ICUE e le informazioni sensibili non classificate trattate e conservate dalle istituzioni e dagli organi dell'Unione, il principio di sussidiarietà non si applica.

- **Proporzionalità**

L'istituzione di una base comune di riferimento per la sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione è necessaria per contribuire a un'amministrazione indipendente ed efficace.

Conformemente al principio di proporzionalità di cui all'articolo 5, paragrafo 4, TUE, le disposizioni del regolamento non sono eccessivamente prescrittive e lasciano spazio a diversi livelli di azione specifica, in linea con il grado di maturità di sicurezza di ogni istituzione e organo dell'Unione.

Inoltre, la soluzione ha un impatto limitato sui diritti fondamentali delle persone. Pertanto, la proposta non va al di là di quanto necessario per affrontare il problema della mancanza di un insieme comune di norme di sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione.

- **Scelta dell'atto giuridico**

Un regolamento basato sull'articolo 298 TFUE è considerato lo strumento giuridico appropriato.

Questo è giustificato dalla prevalenza di elementi che richiedono un'applicazione uniforme che non lasci margini di attuazione alle istituzioni e agli organi dell'Unione e che crei un quadro orizzontale minimo.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Valutazioni ex post / Vaglio di adeguatezza della legislazione vigente**

Non applicabile

- **Consultazioni dei portatori di interessi**

La Commissione ha effettuato un'ampia consultazione dei principali portatori di interessi su vari aspetti relativi alle norme di sicurezza delle informazioni delle istituzioni e degli organi dell'Unione. L'obiettivo generale delle attività di consultazione era raccogliere contributi pertinenti per la preparazione di un'iniziativa legislativa su norme di sicurezza delle informazioni comuni a tutte le istituzioni e tutti gli organi dell'Unione. Le consultazioni intendevano raccogliere contributi su:

- problemi connessi al quadro esistente in materia di sicurezza delle informazioni in seno alle istituzioni e agli organi dell'Unione, che secondo i portatori di interessi dovrebbero essere affrontati nell'ambito dell'iniziativa;
- pertinenza, efficacia, efficienza e valore aggiunto dell'iniziativa;
- impatti previsti dell'iniziativa e altre eventuali conseguenze per i portatori di interessi.

In preparazione della presente proposta legislativa, la Commissione ha consultato le seguenti categorie di portatori di interessi:

1. istituzioni, organi e organismi dell'Unione;
2. autorità di sicurezza nazionali degli Stati membri;
3. esperti del JRC nel campo della ricerca.

Data la specificità della presente iniziativa, che si applica esclusivamente alle istituzioni e agli organi dell'Unione, con un impatto minimo sui cittadini e sulle imprese europei, i servizi della Commissione hanno scelto di dare priorità alla raccolta di punti di vista dei pertinenti gruppi di portatori di interessi. Pertanto **non è stata condotta alcuna consultazione pubblica** specificamente per la presente iniziativa legislativa.

Nel corso del processo di consultazione, i servizi della Commissione hanno utilizzato i **seguenti metodi e forme di consultazione**:

1. opportunità per tutti i portatori di interessi di fornire un riscontro sulla valutazione d'impatto iniziale attraverso la piattaforma "Dì la tua" della Commissione;
2. questionario mirato rivolto agli esperti in materia di sicurezza delle informazioni in seno alle istituzioni e agli organi dell'Unione attraverso un'indagine online dell'UE;
3. questionario mirato rivolto alle autorità di sicurezza nazionali degli Stati membri attraverso un'indagine online dell'UE;

4. una richiesta di valutazione del rischio su misura delle risorse essenziali per la sicurezza delle informazioni, e

5. numerose riunioni e scambi con gli omologhi di istituzioni, organi e organismi, nonché con le autorità di sicurezza nazionali degli Stati membri.

Come contributo principale delle attività di consultazione, la Commissione sottolinea quanto segue:

- la frammentazione dei quadri giuridici pertinenti tra le nostre istituzioni e i nostri organi crea una notevole duplicazione degli sforzi per la creazione e il mantenimento di norme interne e pratiche non interoperabili per trattare le informazioni. Per gli Stati membri, la diversità di tali norme aumenta il rischio di fraintendimenti, interpretazioni errate e non conformità;
- la definizione di una base di riferimento per la sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione creerebbe un ecosistema con norme di sicurezza standardizzate e migliori pratiche, tuttavia occorre tenere conto della diversità e del diverso contesto operativo di ogni istituzione e organo dell'Unione e consentire soluzioni locali;
- la presente iniziativa deve rispettare l'autonomia e i diversi gradi di maturità di sicurezza delle istituzioni e degli organi dell'Unione, che rimarranno pienamente responsabili della loro organizzazione della sicurezza delle informazioni.

- **Assunzione e uso di perizie**

La Commissione ha utilizzato le proprie risorse per svolgere la consultazione dei portatori di interessi. La direzione Sicurezza della DG HR ha svolto i relativi lavori sui sondaggi, le videoconferenze e altri seminari. Questo compito ha comportato sia la selezione dei partecipanti che l'organizzazione di eventi e il trattamento dei contributi ricevuti.

Il Centro comune di ricerca (JRC) ha effettuato una valutazione dei rischi delle principali risorse in materia di sicurezza delle informazioni, utilizzata come base per l'analisi d'impatto.

- **Valutazione d'impatto**

La presente iniziativa è rivolta esclusivamente alle istituzioni e agli organi dell'Unione e ha un impatto limitato per gli Stati membri e le persone. Pertanto, non è stato necessario effettuare una valutazione d'impatto approfondita in quanto non vi erano impatti chiaramente identificabili o significativi sui cittadini e sulle imprese. Una tabella di marcia completa è stata pubblicata sul sito web Europa e ha raccolto i contributi dei portatori di interessi.

- **Efficienza normativa e semplificazione**

Non applicabile

- **Diritti fondamentali**

L'UE si è impegnata a garantire elevati livelli di protezione dei diritti fondamentali. La presente iniziativa garantisce il pieno rispetto dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea[10], come segue:

- Diritto ad una buona amministrazione[11]

[10] Carta dei diritti fondamentali dell'Unione europea (GU C 326 del 26.10.2012, pag. 391).

[11] Articolo 41 della Carta dei diritti fondamentali dell'Unione europea.

Migliorando la sicurezza delle informazioni che trattano quando si occupano delle questioni dei cittadini europei, le istituzioni e gli organi dell'Unione contribuiscono alla realizzazione del principio di buona amministrazione.

- Protezione dei dati di carattere personale[12]

Tutti i trattamenti di dati personali nel quadro della presente proposta sarebbero effettuati in ambienti di fiducia e nel pieno rispetto del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

- Diritto d'accesso ai documenti[13]

L'accesso del pubblico alle ICUE e ai documenti sensibili non classificati rimane pienamente disciplinato dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio.

- Diritto di proprietà intellettuale[14]

Durante il trattamento e la conservazione di informazioni non classificate e ICUE, le istituzioni e gli organi dell'Unione proteggono la proprietà intellettuale conformemente alla direttiva n. 2001/29/CE del Parlamento europeo e del Consiglio[15].

- Libertà di espressione e d'informazione[16]

Sebbene tutti abbiano la libertà di ricevere e condividere informazioni e idee senza interferenze da parte dell'autorità pubblica, ciò non impedisce all'Unione di stabilire le condizioni per l'accesso, il trattamento e la conservazione di determinati tipi di informazioni, sulla base del loro livello di riservatezza.

L'esercizio di tali libertà può essere soggetto a condizioni e restrizioni previste dalla legge e necessarie in una società democratica, al fine di impedire la divulgazione di informazioni ricevute in via riservata e nell'interesse della sicurezza dell'UE.

4. INCIDENZA SUL BILANCIO

La presente proposta richiede l'assegnazione di un funzionario AD e di un assistente AST per il segretariato permanente del gruppo di coordinamento, fornito dalla Commissione, in seno alla direzione Sicurezza della direzione generale Risorse umane e sicurezza.

Per le istituzioni e gli organi si prevedono risparmi sui costi in termini di compiti condivisi e collaborativi e di prevenzione di potenziali danni economici derivanti da incidenti di sicurezza, dovuti a miglioramenti nella sicurezza delle informazioni. Gli sforzi finanziari richiesti per l'attuazione della nuova legislazione possono essere coperti nell'ambito dei programmi di miglioramento della sicurezza delle informazioni esistenti in ogni istituzione e organo dell'Unione.

---

12 Articolo 8 della Carta dei diritti fondamentali dell'Unione europea.

13 Articolo 42 della Carta dei diritti fondamentali dell'Unione europea.

14 Articolo 17 della Carta dei diritti fondamentali dell'Unione europea.

15 Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (GU L 167 del 22.6.2001, pag. 10).

16 Articolo 11 della Carta dei diritti fondamentali dell'Unione europea.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La proposta prevede l'obbligo per la Commissione di riferire ogni tre anni al Parlamento europeo e al Consiglio in merito all'attuazione del regolamento, compreso il funzionamento della governance istituita dal regolamento stesso.

Inoltre, ogni cinque anni, la Commissione valuta il regolamento per esaminarne i risultati effettivi e, su tale base, per stabilire se occorra modificare la legislazione.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

La presente proposta si articola attorno ai requisiti per il trattamento e la conservazione delle informazioni non classificate e delle ICUE, che costituiscono l'oggetto principale dell'iniziativa, la quale mira a rafforzarne la protezione.

Oggetto e ambito di applicazione (articoli 1 e 2)

Il regolamento è inteso a creare un insieme minimo di norme di sicurezza delle informazioni applicabili a tutte le istituzioni e tutti gli organi dell'Unione.

Esso si applica a tutte le informazioni trattate e conservate dalle istituzioni e dagli organi dell'Unione, comprese le informazioni riguardanti le attività della Comunità europea dell'energia atomica diverse dalle informazioni classificate Euratom. Il regolamento disciplina sia le informazioni non classificate che le ICUE.

Definizioni e principi generali (articoli da 3 a 5)

Le definizioni di cui all'articolo 3 si basano sulle norme vigenti in materia di sicurezza delle informazioni adottate separatamente dalle istituzioni e dagli organi dell'Unione.

Oltre ai principi generali della legislazione dell'Unione, vale a dire trasparenza, proporzionalità, efficienza e responsabilità, il regolamento stabilisce le principali linee guida vincolanti, quali la procedura distinta di gestione del rischio di sicurezza delle informazioni applicata da ogni istituzione e organo dell'Unione e la valutazione delle loro informazioni affinché siano categorizzate adeguatamente.

Governance e organizzazione della sicurezza (articoli da 6 a 8)

Tutte le istituzioni e tutti gli organi dell'Unione cooperano in seno a un gruppo di coordinamento interistituzionale per la sicurezza delle informazioni, che delibera per consenso e nell'interesse comune delle istituzioni e degli organi dell'Unione.

Il gruppo di coordinamento riunisce le autorità di sicurezza di tutte le istituzioni e tutti gli organi ed elabora documenti di orientamento sull'attuazione del regolamento. Intrattiene contatti regolari con le autorità di sicurezza nazionali degli Stati membri, riunite in un comitato per la sicurezza delle informazioni.

Sono istituiti cinque sottogruppi composti da esperti che rappresentano diverse istituzioni e organi al fine di razionalizzare le procedure e altri aspetti pratici relativi alla sicurezza delle informazioni.

Ogni istituzione e organo dell'Unione è tenuto a designare un'autorità di sicurezza, che è responsabile di definire le politiche interne di sicurezza delle informazioni e di attuarle. L'autorità di sicurezza stabilisce funzioni specifiche quali l'autorità per la garanzia di sicurezza delle informazioni, l'autorità operativa per la garanzia di sicurezza delle informazioni, l'autorità di accreditamento di sicurezza, l'autorità TEMPEST, l'autorità di approvazione degli apparati crittografici e l'autorità di distribuzione degli apparati

crittografici, che possono essere delegate a un'altra istituzione o un altro organo per motivi di efficienza o di risorse.

Garanzia di sicurezza delle informazioni e sistemi di comunicazione e informazione (articoli da 9 a 11)

Il regolamento istituisce un sottogruppo sulla garanzia di sicurezza delle informazioni, con l'obiettivo di migliorare la coerenza nelle istituzioni e negli organi dell'Unione tra le norme di sicurezza delle informazioni e la base di riferimento per la cibersicurezza quale definita dal regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.

Le istituzioni e gli organi dell'Unione sono tenuti a rispettare i principi menzionati in tali articoli e ad adottare norme interne distinte per specifiche misure di sicurezza, adeguate al proprio ambiente di sicurezza.

Informazioni non classificate (articoli da 12 a 17 e allegato I)

Il regolamento prevede tre categorie di informazioni non classificate: informazioni ad uso pubblico, informazioni normali e informazioni sensibili non classificate. Tutte le categorie sono definite; sono inoltre stabiliti i contrassegni e le condizioni di trattamento per proteggere tali informazioni.

Al fine di coordinare le operazioni di equivalenza tra le particolari categorie stabilite da alcune istituzioni e alcuni organi dell'Unione e le categorie comuni previste dal regolamento, la proposta istituisce un sottogruppo sulle informazioni non classificate.

ICUE (articoli da 18 a 58 e allegati da II a VI)

Essendo il più voluminoso della proposta, questo capo è strutturato in sette sezioni, come segue: disposizioni generali, sicurezza del personale, sicurezza materiale, gestione delle ICUE, protezione delle ICUE nei sistemi di comunicazione e informazione, sicurezza industriale e condivisione di ICUE e scambio di informazioni classificate.

La sezione relativa alle disposizioni generali prevede quattro livelli di ICUE: TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL e RESTREINT UE/EU RESTRICTED e impone l'obbligo per le istituzioni e gli organi dell'Unione di adottare le misure di sicurezza necessarie in base ai risultati di una procedura di gestione del rischio di sicurezza delle informazioni.

Ciascuna delle altre sezioni si concentra sulle norme di protezione delle ICUE, in funzione del settore specifico considerato. Le modalità di tale protezione delle ICUE sono specificate negli allegati da II a V. L'allegato VI contiene la tabella di equivalenza delle ICUE con le classificazioni di sicurezza degli Stati membri e della Comunità europea dell'energia atomica.

Al fine di razionalizzare le pertinenti procedure nel settore ed evitare la duplicazione degli sforzi, il regolamento istituisce il sottogruppo sulla garanzia di sicurezza delle informazioni, il sottogruppo sulle informazioni non classificate, il sottogruppo sulla sicurezza materiale, il sottogruppo sull'accreditamento dei sistemi di comunicazione e informazione che trattano e conservano ICUE e il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate.

Disposizioni finali (articoli da 59 a 62)

Le disposizioni finali assicurano la transizione dalle norme e procedure attuali al nuovo quadro giuridico stabilito dal regolamento. Esse riguardano le norme interne di sicurezza delle informazioni attualmente applicabili nelle istituzioni e negli organi dell'Unione, il riconoscimento delle visite di valutazione effettuate prima dell'inizio dell'applicazione del

regolamento, il trattamento delle intese amministrative concluse in precedenza e il mantenimento dei quadri di sicurezza specifici applicabili alle convenzioni di sovvenzione.

Il regolamento si applica dopo due anni dalla data di entrata in vigore.

2022/0084 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 298,

visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 106 bis,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

1) Le istituzioni e gli organi dell'Unione hanno attualmente le proprie norme di sicurezza delle informazioni basate sul proprio regolamento interno o atto istitutivo, oppure non ne hanno affatto. In tale contesto, ogni istituzione e organo dell'Unione investe molte energie in approcci diversi, con la conseguenza che lo scambio di informazioni non è sempre affidabile. La mancanza di un approccio comune impedisce l'uso di strumenti comuni basati su una serie concordata di norme in funzione delle esigenze di sicurezza delle informazioni da proteggere.

2) Sebbene siano stati compiuti progressi verso norme più coerenti per la protezione delle informazioni classificate UE ("ICUE") e delle informazioni non classificate, l'interoperabilità dei pertinenti sistemi rimane limitata, ostacolando la fluidità del trasferimento delle informazioni tra le diverse istituzioni e i diversi organi dell'Unione. Sono pertanto opportuni ulteriori sforzi per consentire un approccio interistituzionale alla condivisione delle ICUE e delle informazioni sensibili non classificate, con categorie comuni di informazioni e con principi fondamentali di trattamento comuni. Si dovrebbe inoltre prevedere una base di riferimento per semplificare le procedure di condivisione delle ICUE e delle informazioni sensibili non classificate tra le istituzioni e gli organi dell'Unione e con gli Stati membri.

3) È pertanto opportuno stabilire norme pertinenti che assicurino un livello comune di sicurezza delle informazioni in tutte le istituzioni e tutti gli organi dell'Unione. Esse dovrebbero costituire un quadro generale completo e coerente per la protezione delle ICUE e delle informazioni non classificate e garantire l'equivalenza dei principi di base e delle norme minime.

4) La recente pandemia ha provocato un cambiamento significativo nelle prassi di lavoro, facendo diventare gli strumenti di comunicazione remota la regola. Molte procedure che, almeno in parte, erano ancora cartacee sono state quindi rapidamente adattate per permettere il trattamento e lo scambio di informazioni per via elettronica. Questi

sviluppi richiedono modifiche nel trattamento e nella protezione delle informazioni. Il presente regolamento tiene conto delle nuove prassi di lavoro.

5) Creando un livello minimo comune di protezione delle ICUE e delle informazioni non classificate, il presente regolamento contribuisce ad assicurare che le istituzioni e gli organi dell'Unione abbiano il sostegno di un'amministrazione efficace e indipendente nell'assolvimento dei loro compiti. Nel contempo, ogni istituzione e organo dell'Unione conserva la propria autonomia nel determinare le modalità di attuazione delle norme stabilite nel presente regolamento, in linea con le proprie esigenze di sicurezza. Il presente regolamento non impedisce in alcun caso alle istituzioni e agli organi dell'Unione di assolvere i propri compiti, quali conferiti dalla legislazione dell'UE, né viola la loro autonomia istituzionale.

6) Il presente regolamento non pregiudica il regolamento n. 3/1958[17], il regolamento n. 31 (CEE), n. 11 (CEEA), relativo allo statuto dei funzionari e al regime applicabile agli altri agenti della Comunità Economica Europea e della Comunità Europea dell'Energia Atomica[18], il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[19], il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[20], il regolamento (CEE, Euratom) n. 354/83 del Consiglio[21], il regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio[22], il regolamento (UE) 2021/697 del Parlamento europeo e del Consiglio[23] e il regolamento (UE) [...] del Parlamento europeo e del Consiglio[24] che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.

7) Al fine di preservare la natura specifica delle attività della Comunità europea dell'energia atomica disciplinate dal regolamento n. 3/1958 del Consiglio della Comunità europea dell'energia atomica[25], il presente regolamento non dovrebbe applicarsi alle informazioni classificate Euratom. Tuttavia, tutte le informazioni riguardanti altre attività Euratom non contemplate dal regolamento n. 3/1958 dovrebbero rientrare nell'ambito di applicazione del presente regolamento.

---

17 Regolamento (Euratom) n. 3/1958 relativo all'applicazione dell'articolo 24 del Trattato che istituisce la Comunità Europea dell'Energia Atomica (GU 17 del 6.10.1958, pag. 406).

18 GU L 45 del 14.6.1962, pag. 1385.

19 Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

20 Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39)

21 Regolamento (CEE, Euratom) n. 354/83 del Consiglio, del 1o febbraio 1983, che rende accessibili al pubblico gli archivi storici della Comunità economica europea e della Comunità europea dell'energia atomica (GU L 43 del 15.2.1983, pag. 1).

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

23 Regolamento (UE) 2021/697 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il Fondo europeo per la difesa e abroga il regolamento (UE) 2018/1092 (GU L 170 del 12.5.2021, pag. 149).

24 Regolamento (UE) [...] del Parlamento europeo e del Consiglio che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, da adottare.

25 Consiglio CEEA: regolamento n. 3 relativo all'applicazione dell'articolo 24 del Trattato che istituisce la Comunità Europea dell'Energia Atomica (GU 17 del 6.10.1958, pag. 406).

8) Al fine di creare una struttura formale per la cooperazione tra le istituzioni e gli organi dell'Unione nel settore della sicurezza delle informazioni, occorre istituire un gruppo di coordinamento interistituzionale ("gruppo di coordinamento") in cui siano rappresentate tutte le autorità di sicurezza delle istituzioni e degli organi dell'Unione. Senza essere dotato di poteri decisionali, il gruppo di coordinamento dovrebbe migliorare la coerenza delle politiche nel settore della sicurezza delle informazioni e contribuire all'armonizzazione delle procedure e degli strumenti per la sicurezza delle informazioni in tutte le istituzioni e tutti gli organi dell'Unione.

9) Il lavoro del gruppo di coordinamento necessita del sostegno di esperti in diversi settori della sicurezza delle informazioni: categorizzazione e apposizione di un contrassegno, sistemi di comunicazione e informazione, accreditamento, sicurezza materiale e condivisione di ICUE e scambio di informazioni classificate. Al fine di evitare la duplicazione degli sforzi tra le istituzioni e gli organi dell'Unione, dovrebbero essere istituiti sottogruppi tematici. Inoltre, ove necessario, il gruppo di coordinamento dovrebbe poter istituire altri sottogruppi con compiti specifici.

10) Il gruppo di coordinamento dovrebbe cooperare strettamente con le autorità di sicurezza nazionali degli Stati membri allo scopo di rafforzare la sicurezza delle informazioni nell'Unione. È pertanto opportuno istituire un comitato degli Stati membri per la sicurezza delle informazioni, incaricato di fornire consulenza al gruppo di coordinamento.

11) Benché le entità comuni che rappresentano tutte le istituzioni e tutti gli organi dell'Unione siano istituite in base al principio di cooperazione, ogni istituzione e organo dell'Unione dovrebbe rimanere pienamente responsabile della sicurezza delle informazioni al proprio interno. Ogni istituzione e organo dell'Unione dovrebbe disporre di un'autorità di sicurezza e, se necessario, di altre autorità incaricate di responsabilità specifiche in materia di sicurezza delle informazioni.

12) Il principio della gestione dei rischi relativi alla sicurezza delle informazioni dovrebbe essere al centro della politica che ogni istituzione e organo dell'Unione deve sviluppare in questo settore. Sebbene debbano essere soddisfatti i requisiti minimi previsti dal presente regolamento, ogni istituzione e organo dell'Unione dovrebbe adottare misure di sicurezza specifiche per proteggere le informazioni conformemente ai risultati di una valutazione interna del rischio. Analogamente, i mezzi tecnici per proteggere le informazioni dovrebbero essere adattati alla situazione specifica di ogni istituzione e organo.

13) Data la diversità delle categorie di informazioni non classificate che le istituzioni e gli organi dell'Unione hanno sviluppato sulla base delle proprie norme di sicurezza delle informazioni, e al fine di evitare ritardi nell'attuazione del presente regolamento, le istituzioni e gli organi dell'Unione dovrebbero poter mantenere il proprio sistema di contrassegni a fini interni o quando scambiano informazioni con i propri particolari omologhi di altre istituzioni e organi dell'Unione o degli Stati membri.

14) Onde adeguarsi alle nuove prassi di telelavoro, le reti per la connessione ai servizi di accesso remoto dell'istituzione o dell'organo dell'Unione dovrebbero essere protette mediante misure di sicurezza adeguate.

15) Poiché le istituzioni e gli organi dell'Unione ricorrono spesso a contraenti e all'esternalizzazione, è importante stabilire disposizioni comuni sul personale dei contraenti che svolge compiti correlati alla sicurezza delle informazioni.

16) Le disposizioni sostanziali relative all'accesso alle ICUE previste dalle norme interne di varie istituzioni e vari organi dell'Unione sono attualmente allineate, ma vi sono differenze significative per quanto riguarda le denominazioni e le procedure richieste. Ciò comporta un onere per le autorità di sicurezza nazionali degli Stati membri, che devono adeguarsi a requisiti diversi. È pertanto necessario prevedere un glossario comune e procedure comuni nel settore della sicurezza del personale, in modo da semplificare la cooperazione con le autorità di sicurezza nazionali degli Stati membri e limitare il rischio di compromissione delle ICUE.

17) Data la disparità di risorse tra istituzioni e organi dell'Unione e al fine di razionalizzare le loro procedure e prassi pertinenti, i compiti relativi al nulla osta di sicurezza possono essere affidati alla Commissione onde proseguire una prassi consolidata nel settore del nulla osta di sicurezza e contribuire alla centralizzazione dei compiti assegnati a ogni autorità di sicurezza.

18) La protezione delle ICUE è assicurata anche mediante misure tecniche e organizzative che si applicano ai locali, agli edifici, alle sale, agli uffici o alle strutture delle istituzioni e degli organi dell'Unione in cui le ICUE sono discusse, trattate o conservate. Il presente regolamento prevede l'attuazione di una procedura di gestione della sicurezza delle informazioni nel settore della sicurezza materiale che consentirebbe alle istituzioni e agli organi dell'Unione di scegliere le misure di sicurezza adeguate per i loro siti.

19) Tutte le istituzioni e tutti gli organi dell'Unione che trattano e conservano ICUE dovrebbero predisporre nei loro siti zone oggetto di protezione materiale, al fine di garantire lo stesso livello di protezione per i pertinenti livelli di classifica ICUE trattati e conservati all'interno. Tali zone dovrebbero essere designate come zone amministrative e zone protette e rispettare norme minime comuni per la protezione delle ICUE.

20) Il controllo dell'originatore è un principio importante nella gestione delle ICUE, pertanto esso deve essere chiaramente stabilito e sviluppato. A tale riguardo, la creazione di ICUE conferisce all'originatore una responsabilità che dovrebbe coprire l'intero ciclo di vita del pertinente documento ICUE.

21) Le istituzioni e gli organi dell'Unione tradizionalmente hanno sviluppato i propri sistemi di comunicazione e informazione per lo più in modo autonomo, senza prestare sufficiente attenzione alla loro interoperabilità in tutte le istituzioni e tutti gli organi dell'Unione. Occorre pertanto stabilire requisiti minimi di sicurezza relativi ai sistemi di comunicazione e informazione ("CIS") che trattano e conservano sia ICUE che informazioni non classificate, allo scopo di garantire uno scambio fluido delle informazioni con le pertinenti parti interessate.

22) Al fine di stabilire una norma di accreditamento unica dei CIS che trattano e conservano ICUE, le istituzioni e gli organi dell'Unione dovrebbero collaborare in un gruppo istituito a tale scopo. Si raccomanda che tutte le istituzioni e tutti gli organi dell'Unione utilizzino tale norma per contribuire a un livello generale di protezione delle ICUE. Tuttavia, per quanto riguarda l'autonomia organizzativa, la decisione spetta all'autorità competente di ogni istituzione od organo.

23) Tutte le istituzioni e tutti gli organi dell'Unione dovrebbero seguire le stesse procedure e applicare le stesse misure quando aggiudicano e attuano contratti o convenzioni di sovvenzione classificati. È pertanto necessario stabilire chiaramente sia gli elementi obbligatori che quelli facoltativi di un contratto e di una convenzione di sovvenzione

classificati. Tuttavia le misure per la protezione delle ICUE in relazione ai contratti e alle convenzioni di sovvenzione classificati dovrebbero tenere conto delle norme già sviluppate separatamente in questo settore dalle istituzioni e dagli organi dell'Unione insieme agli Stati membri.

24) La stretta cooperazione tra le istituzioni e gli organi dell'Unione e la molteplicità di sinergie sviluppate tra di essi comportano la condivisione di una grande quantità di informazioni. Ai fini della sicurezza delle informazioni classificate, l'onestà di un'istituzione o un organo dell'Unione dovrebbe essere valutata prima che l'istituzione o l'organo in questione tratti e conservi un livello specifico di ICUE.

25) Inoltre, anche la condivisione di ICUE tra le istituzioni e gli organi dell'Unione e lo scambio di informazioni classificate con organizzazioni internazionali e paesi terzi dovrebbero essere disciplinati da misure di sicurezza adeguate per la protezione di tali informazioni. Quando sono previsti accordi sulla sicurezza delle informazioni, si applicano le disposizioni dell'articolo 218 del trattato.

26) Gli accordi sulla sicurezza delle informazioni sono intesi a garantire il quadro giuridico generale per lo scambio di informazioni classificate dell'Unione con paesi terzi e organizzazioni internazionali, tuttavia è necessario prevedere anche la possibilità per le istituzioni e gli organi dell'Unione di concludere intese amministrative con un omologo specifico di un paese terzo o di un'organizzazione internazionale per lo scambio di ICUE.

27) Il presente regolamento stabilisce un quadro comune a tutte le istituzioni e tutti gli organi dell'Unione. Al fine di evitare di imporre alle istituzioni e agli organi dell'Unione un onere amministrativo eccessivo nel processo di adeguamento delle loro norme di sicurezza interne alle norme stabilite dal presente regolamento, quest'ultimo dovrebbe applicarsi a decorrere da due anni dopo l'entrata in vigore.

28) In conformità dei punti 22 e 23 dell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[26], la Commissione dovrebbe valutare il presente regolamento per valutarne gli effetti concreti e la necessità di un'azione ulteriore. Al più tardi tre anni dopo la data di applicazione del presente regolamento, la Commissione dovrebbe presentare al Parlamento europeo e al Consiglio una relazione sulla sua attuazione.

29) Conformemente all'articolo 42 del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[27], il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il […],

---

[26] Accordo interistituzionale "Legiferare meglio" tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea (GU L 123 del 12.5.2016, pag. 1).

[27] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo 1
Disposizioni generali

Articolo 1

Oggetto

1. Il presente regolamento stabilisce le norme di sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica a tutte le informazioni trattate e conservate dalle istituzioni e dagli organi dell'Unione, comprese le informazioni riguardanti le attività della Comunità europea dell'energia atomica diverse dalle informazioni classificate Euratom.

2. Esso si applica ai seguenti livelli di riservatezza delle informazioni:

   a) tre livelli di informazioni non classificate: informazioni ad uso pubblico, informazioni normali e informazioni sensibili non classificate;

   b) quattro livelli di informazioni classificate UE: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

3. Questi livelli si basano sul danno che la divulgazione non autorizzata può arrecare ai legittimi interessi privati e pubblici, compresi quelli dell'Unione, delle istituzioni e degli organi dell'Unione, degli Stati membri o di altre parti interessate, in modo che possano essere applicate le misure di protezione adeguate.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

   a) "informazioni": qualsiasi dato in forma orale, visiva, elettronica, magnetica o materiale, o sotto forma di materiale, attrezzature o tecnologie, comprese riproduzioni, traduzioni e materiale in corso di elaborazione;

   b) "sicurezza delle informazioni": la garanzia dell'autenticità, della disponibilità, della riservatezza, dell'integrità e della non disconoscibilità delle informazioni;

   c) "trattamento" delle informazioni: qualsiasi azione di cui possono essere oggetto le informazioni nel loro ciclo di vita; ciò comprende la loro creazione, raccolta, registrazione, assegnazione di un livello di riservatezza, elaborazione, visualizzazione, consultazione, trasporto, trasmissione, declassamento, declassificazione, archiviazione e distruzione;

   d) "conservazione": l'atto di custodire le informazioni su qualsiasi supporto per garantirne la disponibilità per un uso futuro;

e) "istituzioni e organi dell'Unione": le istituzioni, gli organi e gli organismi dell'Unione istituiti dal trattato sull'Unione europea, dal trattato sul funzionamento dell'Unione europea, dal trattato che istituisce la Comunità europea dell'energia atomica o da un atto legislativo, oppure sulla base dei medesimi;

f) "informazioni classificate Euratom": le informazioni ai sensi del regolamento n. 3/1958 del Consiglio della Comunità europea dell'energia atomica;

g) "autorità di sicurezza": la funzione di sicurezza di ogni istituzione e organo dell'Unione, designata conformemente al rispettivo regolamento interno o atto istitutivo;

h) "procedura di gestione del rischio di sicurezza delle informazioni": 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 sistema in uso; essa contempla tutte le attività correlate al rischio, tra cui la valutazione, il trattamento, l'accettazione e la comunicazione;

i) "risorsa": qualsiasi cosa che ha valore per un'istituzione o un organo dell'Unione, le sue operazioni e la loro continuità, comprese le risorse dell'informazione che sostengono la sua missione;

j) "procedure operative di sicurezza": una serie di procedure documentate, quali indicate nell'allegato III, per il funzionamento di una zona protetta, di un sistema di comunicazione e informazione o di altre risorse o servizi connessi alla sicurezza, al fine di garantirne l'efficacia;

k) "sistema di comunicazione e informazione" o "CIS": ogni sistema che consente il trattamento e la conservazione delle informazioni in forma elettronica, compreso l'insieme delle risorse necessarie al suo funzionamento;

l) "garanzia di sicurezza delle informazioni": la certezza che i sistemi di comunicazione e informazione proteggeranno le informazioni che trattano e conservano, e funzioneranno nel modo dovuto e a tempo debito sotto il controllo degli utenti legittimi, garantendo nel contempo gli adeguati livelli di autenticità, disponibilità, riservatezza, integrità e non disconoscibilità;

m) "accreditamento": l'autorizzazione formale accordata dall'autorità di accreditamento di sicurezza a un sistema di comunicazione e informazione o a una zona protetta per, rispettivamente, il trattamento o la conservazione di un livello di classifica predeterminato di ICUE;

n) "procedura di accreditamento": le fasi e i compiti richiesti prima dell'accreditamento;

o) "misure di sicurezza TEMPEST": le misure volte a proteggere i CIS che trattano e conservano informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore in modo tale che tali informazioni non possano essere compromesse da radiazioni elettromagnetiche non intenzionali;

p) "CERT-UE": il centro per la cibersicurezza delle istituzioni e degli organi dell'Unione ai sensi del regolamento (UE) [...] del Parlamento europeo e del Consiglio che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione;

q) "incidente di sicurezza delle informazioni": qualsiasi evento che potenzialmente compromette l'autenticità, la disponibilità, la riservatezza, l'integrità o la non disconoscibilità delle informazioni conservate, trasmesse o trattate;

r) "necessità di conoscere": la necessità di una persona di accedere a specifiche informazioni trattate o conservate da un'istituzione o un organo dell'Unione per assolvere i compiti di tale istituzione o organo dell'Unione;

s) "zero trust": un modello di sicurezza, una serie di principi di progettazione dei sistemi e una strategia coordinata di cibersicurezza e di gestione dei sistemi, basati sul riconoscimento dell'esistenza di minacce all'interno e all'esterno dei confini di rete tradizionali;

t) "contrassegno": un'etichetta apposta alle informazioni per garantire l'applicazione delle misure di sicurezza adeguate;

u) "contrassegno di sicurezza": un contrassegno indicante il livello di riservatezza delle informazioni;

v) "contrassegno di distribuzione": un contrassegno indicante i destinatari previsti delle informazioni all'interno dell'istituzione o dell'organo dell'Unione di origine;

w) "contrassegno di divulgabilità": un contrassegno indicante i destinatari ammessi al di fuori dell'istituzione o dell'organo dell'Unione di origine;

x) "proprietario del sistema": la persona responsabile del complesso degli appalti, dello sviluppo, dell'integrazione, della modifica, del funzionamento, della manutenzione e del ritiro di un sistema di comunicazione e informazione;

y) "minaccia per la sicurezza delle informazioni": un evento o agente che presumibilmente, in mancanza di una reazione che lo ponga sotto controllo, compromette la sicurezza delle informazioni;

z) "vulnerabilità": un punto debole, una suscettibilità o un difetto di una risorsa, di un sistema, di un processo o di un controllo che possono essere sfruttati da una o più minacce;

aa) "rischio": il potenziale effetto negativo di una determinata minaccia che sfrutti le vulnerabilità interne ed esterne di un'istituzione o un organo dell'Unione o dei sistemi da essa o esso utilizzati arrecando danni ai legittimi interessi privati e pubblici, calcolato come una combinazione tra le probabilità del verificarsi delle minacce e il loro impatto;

ab) "rischio residuo": il rischio che resta una volta attuate le misure di sicurezza;

ac) "valutazione del rischio": l'identificazione delle minacce e delle vulnerabilità e l'esecuzione delle relative analisi del rischio, ossia l'analisi della probabilità e dell'impatto;

ad) "trattamento del rischio": mitigazione, rimozione, riduzione (tramite un'opportuna combinazione di misure tecniche, materiali, organizzative o procedurali), trasferimento o controllo del rischio.

ae) "certificato europeo di cibersicurezza": un certificato ai sensi dell'articolo 2, punto 11, del regolamento (UE) 2019/881[28];

af) "detentore": una persona debitamente autorizzata con una necessità di conoscere stabilita, che detiene un elemento di informazione che necessita di protezione ed è di conseguenza responsabile della sua protezione;

ag) "materiale": qualsiasi documento, vettore di dati o elemento di macchinario o attrezzatura, sia sotto forma di prodotto finito sia in corso di lavorazione;

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

ai) "autorizzazione di accesso alle ICUE": una decisione dell'autorità di sicurezza in base alla quale un funzionario o altro agente di un'istituzione o un organo dell'Unione o un esperto nazionale distaccato presso un'istituzione o un organo dell'Unione può avere accesso alle ICUE fino a un livello di classifica specifico per un determinato periodo;

aj) "autorità di sicurezza nazionale" o "NSA": un'autorità pubblica di uno Stato membro che ha la responsabilità finale per la sicurezza delle informazioni classificate in tale Stato membro;

ak) "autorità di sicurezza designata" o "DSA": un'autorità di uno Stato membro (NSA o altra autorità competente) responsabile di fornire guida e assistenza nell'attuazione della sicurezza industriale o nelle procedure di nulla osta, o in entrambe;

al) "indagine di sicurezza": le procedure investigative condotte dall'autorità competente di uno Stato membro conformemente alle disposizioni legislative e regolamentari nazionali volte ad accertare l'inesistenza di informazioni negative note sul conto di una persona che osterebbero alla concessione di un nulla osta di sicurezza fino a un livello specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore);

am) "sicurezza materiale": l'applicazione di misure materiali, tecniche e organizzative ai locali, agli edifici, alle sale, agli uffici o alle strutture di un'istituzione o un organo dell'Unione che necessitano di essere protetti dall'accesso non autorizzato alle informazioni ivi trattate, conservate o discusse;

an) "siti": i locali, gli edifici, le sale, gli uffici o le strutture di un'istituzione o un organo dell'Unione;

ao) "difesa in profondità": un tipo di sicurezza che utilizza più livelli indipendenti di controlli di sicurezza per garantire che qualora uno venga meno un altro sia funzionante;

[28] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

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

aq) "prodotto crittografico": prodotto la cui funzione principale e primaria è la fornitura di servizi di sicurezza (autenticità, disponibilità, riservatezza, integrità e non disconoscibilità) mediante uno o più meccanismi crittografici;

ar) "originatore": istituzione o organo dell'Unione, Stato membro, paese terzo o organizzazione internazionale sotto la cui autorità sono state create o introdotte nelle strutture dell'Unione informazioni classificate;

as) "documento": qualsiasi contenuto, a prescindere dal suo supporto (cartaceo, elettronico, magnetico o di altro tipo), in forma scritta o in una registrazione visiva o audiovisiva;

at) "registrazione a fini di sicurezza": l'applicazione di procedure che registrano il ciclo di vita dei materiali, ivi comprese la diffusione e la distruzione;

au) "declassificazione": la soppressione di qualsiasi classifica di sicurezza;

av) "declassamento": una riduzione del livello di classifica di sicurezza;

aw) "contratto classificato": un contratto quadro o un contratto, conformemente al regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, stipulato da un'istituzione o un organo dell'Unione, con un contraente per la fornitura di beni mobili o immobili, l'esecuzione di lavori o la prestazione di servizi, la cui esecuzione richiede o implica il trattamento, compresa la creazione, o la conservazione di ICUE;

ax) "convenzione di sovvenzione classificata": una convenzione con cui un'istituzione o un organo dell'Unione concede una sovvenzione, come stabilito nel titolo VIII, del regolamento (UE, Euratom) 2018/1046, la cui esecuzione richiede o implica il trattamento, compresa la creazione, o la conservazione di ICUE;

ay) "subcontratto classificato": un contratto stipulato da un contraente o un beneficiario di un'istituzione o un organo dell'Unione con un subcontraente per la fornitura di beni mobili o immobili, l'esecuzione di lavori o la prestazione di servizi, la cui esecuzione richiede o implica il trattamento, compresa la creazione, o la conservazione di ICUE;

az) "istruzione di sicurezza del programma o progetto" o "PSI": un elenco delle procedure di sicurezza che sono applicate a un programma o progetto specifico per uniformare le procedure di sicurezza;

ba) "lettera sugli aspetti di sicurezza" o "SAL": un pacchetto di condizioni contrattuali specifiche emesso dall'autorità contraente o che eroga la sovvenzione, che è parte integrante di un contratto o una convenzione di sovvenzione classificati implicante l'accesso o la creazione di ICUE e in cui sono individuati i requisiti di sicurezza e gli elementi del contratto o della sovvenzione che richiedono una protezione di sicurezza;

bb) "guida alle classifiche di sicurezza" o "SCG": un documento che illustra gli elementi di un programma, progetto, contratto o convenzione di sovvenzione classificati e precisa i livelli di classifica di sicurezza applicabili.

Articolo 4

Principi generali

1. Ogni istituzione e organo dell'Unione è responsabile dell'attuazione delle disposizioni del presente regolamento al proprio interno, tenuto conto della propria procedura di gestione del rischio di sicurezza delle informazioni.

2. L'inosservanza del presente regolamento, in particolare la divulgazione non autorizzata di informazioni aventi un livello di riservatezza di cui all'articolo 2, paragrafo 2, ad eccezione delle informazioni ad uso pubblico, è oggetto di indagine e può far sorgere la responsabilità del personale conformemente ai trattati o allo statuto del personale applicabile.

3. Le istituzioni e gli organi dell'Unione valutano tutte le informazioni che trattano e che conservano al fine di ordinarle secondo categorie conformemente ai livelli di riservatezza di cui all'articolo 2, paragrafo 2.

4. Le istituzioni e gli organi dell'Unione determinano le esigenze di sicurezza di tutte le informazioni che gestiscono e conservano tenuto conto dei seguenti aspetti:

   a) autenticità: la garanzia che l'informazione è veritiera e proviene da fonti in buona fede;

   b) disponibilità: l'accessibilità e l'utilizzabilità su richiesta di un'entità autorizzata;

   c) riservatezza: la non divulgazione dell'informazione a persone, entità o procedure non autorizzate;

   d) integrità: il fatto che l'informazione è completa e che la completezza dell'informazione non è modificata;

   e) non disconoscibilità: la capacità di provare che un'azione o un evento sono effettivamente accaduti e non possono essere negati in seguito.

5. Per ogni sistema di comunicazione e informazione sotto la loro responsabilità, le istituzioni e gli organi dell'Unione individuano il massimo livello di riservatezza che il sistema di comunicazione e informazione può trattare e conservare, effettuano una valutazione del rischio di sicurezza delle informazioni e monitorano regolarmente le esigenze di sicurezza e la corretta attuazione delle misure di protezione individuate.

6. Tutte le istituzioni e tutti gli organi dell'Unione forniscono attività di formazione e sensibilizzazione sulle modalità di trattamento e conservazione delle informazioni non classificate e delle ICUE.

   Le istituzioni e gli organi dell'Unione che trattano e conservano ICUE organizzano una formazione obbligatoria almeno una volta ogni cinque anni destinata a tutte le persone autorizzate ad accedere alle ICUE. Le istituzioni e gli organi dell'Unione interessati organizzano una formazione specifica per le funzioni specifiche incaricate di compiti riguardanti la sicurezza delle informazioni.

   Un'istituzione o un organo dell'Unione può coordinare tali attività di formazione e sensibilizzazione con altre istituzioni e altri organi dell'Unione.

Articolo 5

Procedura di gestione del rischio di sicurezza delle informazioni

1. Ogni istituzione e organo dell'Unione istituisce una procedura di gestione del rischio di sicurezza delle informazioni per la protezione delle informazioni che tratta e conserva.

2. La procedura di gestione del rischio di sicurezza delle informazioni comprende le seguenti fasi:

   a) identificazione delle minacce e delle vulnerabilità;

   b) valutazione del rischio;

   c) trattamento del rischio;

   d) accettazione del rischio;

   e) comunicazione del rischio.

3. La procedura di gestione del rischio di sicurezza delle informazioni tiene conto di tutti gli elementi pertinenti per l'istituzione o l'organo in questione, in particolare:

   a) il livello di riservatezza delle informazioni e i correlati obblighi giuridici;

   b) la forma e la quantità delle informazioni e le strutture o i CIS in cui le informazioni sono trattate e conservate;

   c) le persone che accedono alle informazioni in sito o da remoto;

   d) l'ambiente circostante e la struttura degli edifici o delle zone in cui sono conservate le informazioni;

   e) le minacce nei confronti dell'Unione, delle istituzioni e degli organi dell'Unione o degli Stati membri derivanti da attacchi informatici, attacchi della catena di approvvigionamento, spionaggio, sabotaggio, attività terroristiche, attività sovversive o altre attività criminali;

   f) la continuità operativa e il ripristino in caso di disastro;

   g) i risultati di ispezioni, audit o visite di valutazione, se del caso.

Capo 2
Governance e organizzazione della sicurezza

Articolo 6

Gruppo di coordinamento interistituzionale per la sicurezza delle informazioni

1. È istituito un gruppo di coordinamento interistituzionale per la sicurezza delle informazioni ("gruppo di coordinamento").

   Esso è composto da tutte le autorità di sicurezza delle istituzioni e degli organi dell'Unione e ha il mandato di definirne la politica comune nel settore della sicurezza delle informazioni.

2. Deliberando per consenso e nell'interesse comune di tutte le istituzioni e tutti gli organi dell'Unione, il gruppo di coordinamento:

   a) adotta il proprio regolamento interno e gli obiettivi e le priorità comuni annuali;

b) adotta decisioni sull'istituzione di sottogruppi tematici e sul loro mandato;

c) elabora documenti di orientamento sull'attuazione del presente regolamento, in cooperazione con il comitato interistituzionale per la cibersicurezza di cui all'articolo 9 del regolamento (UE) [...] che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, se del caso;

d) istituisce apposite piattaforme per la condivisione delle migliori pratiche e delle conoscenze su temi comuni pertinenti per la sicurezza delle informazioni, nonché per l'assistenza in caso di incidenti di sicurezza delle informazioni;

e) assicura il necessario coordinamento delle misure di sicurezza con le competenti autorità di sicurezza nazionali per proteggere le ICUE.

3. Il gruppo di coordinamento designa un presidente e due vicepresidenti tra i suoi membri, per un periodo di tre anni.

4. Il gruppo di coordinamento si riunisce almeno una volta all'anno su iniziativa del presidente o su domanda di un'istituzione o un organo dell'Unione.

5. Il gruppo di coordinamento riceve assistenza amministrativa da un segretariato permanente fornito dalla Commissione.

6. Ogni istituzione od organo dell'Unione è adeguatamente rappresentato nel gruppo di coordinamento e, se del caso, nei sottogruppi tematici.

7. Le istituzioni e gli organi dell'Unione sottopongono all'attenzione del gruppo di coordinamento qualsiasi sviluppo significativo della politica di sicurezza delle informazioni all'interno della propria organizzazione.

8. Nell'adempimento dei compiti di cui al paragrafo 2, lettera e), il gruppo di coordinamento è assistito da un comitato per la sicurezza delle informazioni. Tale comitato è composto da un rappresentante di ogni autorità di sicurezza nazionale ed è presieduto dal segretariato del gruppo di coordinamento di cui al paragrafo 5. Il comitato per la sicurezza delle informazioni svolge un ruolo consultivo.

Articolo 7

Sottogruppi tematici

1. Il gruppo di coordinamento istituisce i seguenti sottogruppi tematici permanenti per facilitare l'attuazione del presente regolamento:

a) un sottogruppo sulla garanzia di sicurezza delle informazioni;

b) un sottogruppo sulle informazioni non classificate:

c) un sottogruppo sulla sicurezza materiale;

d) un sottogruppo sull'accreditamento dei sistemi di comunicazione e informazione che trattano e conservano ICUE;

e) un sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate.

2. Ove necessario, il gruppo di coordinamento può istituire sottogruppi ad hoc per un compito specifico e per una durata limitata.

3. Salvo altrimenti disposto nel loro mandato, i sottogruppi si basano sull'adesione aperta in rappresentanza dell'istituzione o dell'organo dell'Unione in questione. I membri dei sottogruppi sono esperti nei rispettivi settori di competenza.

4. Il segretariato del gruppo di coordinamento di cui all'articolo 5, paragrafo 5, sostiene i lavori di tutti i sottogruppi e assicura la comunicazione tra i loro membri.

Articolo 8

Organizzazione della sicurezza

1. Ogni istituzione e organo dell'Unione designa un'autorità di sicurezza che assume le responsabilità assegnate dal presente regolamento e, se del caso, dalle proprie norme di sicurezza interne. Nell'adempimento dei propri compiti, ogni autorità di sicurezza dispone del sostegno del servizio o funzionario incaricato dei compiti di sicurezza delle informazioni.

2. Ove necessario, l'autorità di sicurezza di ogni istituzione e organo dell'Unione adotta le norme di attuazione interne per la protezione delle informazioni, conformemente ai compiti specifici dell'istituzione o dell'organo in questione, quali conferiti dal diritto dell'UE, e in base alla sua autonomia istituzionale.

3. Ove opportuno, l'autorità di sicurezza assume anche le seguenti funzioni:

   a) autorità per la garanzia di sicurezza delle informazioni, incaricata di sviluppare le politiche di sicurezza della garanzia delle informazioni e gli orientamenti di sicurezza e di monitorare la loro efficacia e pertinenza;

   b) autorità operativa per la garanzia di sicurezza delle informazioni, responsabile dello sviluppo di una documentazione di sicurezza, in particolare le procedure operative di sicurezza e il piano crittografico nell'ambito della procedura di accreditamento del sistema di comunicazione e informazione;

   c) autorità di accreditamento di sicurezza, incaricata di accreditare le zone protette e il CIS che tratta e conserva ICUE;

   d) autorità TEMPEST, responsabile dell'approvazione delle misure adottate per proteggere le ICUE in modo tale che queste non possano essere compromesse da radiazioni elettromagnetiche non intenzionali;

   e) autorità di approvazione degli apparati crittografici, responsabile dell'approvazione dell'uso delle tecnologie di crittografia sulla base di una richiesta del proprietario del sistema;

   f) autorità di distribuzione degli apparati crittografici, responsabile della distribuzione del materiale crittografico utilizzato per la protezione delle ICUE (dispositivi di cifratura, chiavi crittografiche, certificati e relativi autenticatori) agli utenti interessati.

4. Le responsabilità di una o più funzioni di cui al paragrafo 3 possono essere delegate a un'altra istituzione o un altro organo dell'Unione laddove il decentramento della sicurezza offra garanzie di efficienza, risparmio di tempo o di risorse.

Capo 3
Garanzia di sicurezza delle informazioni e sistemi di comunicazione e informazione (CIS)

Articolo 9

Principi di garanzia di sicurezza delle informazioni

1. La valutazione delle esigenze di sicurezza delle informazioni è presa in considerazione sin dall'inizio della creazione o nella fase di appalto per quanto riguarda tutti i CIS, compresi i CIS interni, esternalizzati e ibridi.

2. I CIS che trattano e conservano ICUE sono accreditati conformemente al capo 5, sezione 5. I CIS che trattano e conservano informazioni sensibili non classificate soddisfano i requisiti minimi per le informazioni sensibili non classificate nei CIS, di cui al capo 4.

Articolo 10

Sottogruppo sulla garanzia di sicurezza delle informazioni

1. Il sottogruppo sulla garanzia di sicurezza delle informazioni di cui all'articolo 7, paragrafo 1, lettera a), ha i seguenti ruoli e responsabilità:

   a) fornire orientamenti e migliori pratiche in materia di contrassegni, trattamento e conservazione delle informazioni nei CIS, in stretta cooperazione con il comitato interistituzionale per la cibersicurezza di cui all'articolo 9 del regolamento (UE) [...] che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione;

   b) istituire uno schema di metadati per i contrassegni e tutte le informazioni tecniche necessarie per contribuire a uno scambio interoperabile e fluido delle informazioni in tutte le istituzioni e tutti gli organi dell'Unione quando interconnettono i rispettivi CIS;

   c) contribuire alla coerenza tra le norme di sicurezza delle informazioni e la base di riferimento per la cibersicurezza in tutte le istituzioni e tutti gli organi dell'Unione, di cui all'articolo 5 del regolamento UE [...] che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.

Articolo 11

Requisiti per i sistemi di comunicazione e informazione

1. Le istituzioni e gli organi dell'Unione informano gli utenti in merito ai livelli di riservatezza delle informazioni che possono essere trattati e conservati in un CIS. Se un CIS tratta e conserva più livelli di riservatezza, sono utilizzati metadati e contrassegni visivi per garantire che i diversi livelli possano essere distinti.

2. Le istituzioni e gli organi dell'Unione individuano gli utenti del CIS prima di concedere loro l'accesso a livelli di riservatezza diversi dall'uso pubblico. Gli utenti sono autenticati a un livello di garanzia di sicurezza adeguato al livello di riservatezza. Se del caso, è usato un sistema comune di identificazione sicuro.

3. Sono conservati log di sicurezza adeguati per tutti i CIS al fine di garantire indagini rapide in caso di violazione o fuga di informazioni. Tali log sono conservati per la durata stabilita nella valutazione dell'impatto operativo o nelle pertinenti politiche di sicurezza, in modo non ripudiabile.

   Se un CIS tratta e conserva ICUE, i log relativi alla necessità di conoscere e all'accesso alle informazioni sono conservati fino alla declassificazione delle informazioni. I log di sicurezza sono consultabili e accessibili da parte dell'autorità di sicurezza.

4. Le istituzioni e gli organi dell'Unione adottano norme interne sulla sicurezza dei CIS per specificare le misure di sicurezza adeguate in funzione delle esigenze di sicurezza delle informazioni da trattare e conservare e tenuto conto delle giurisdizioni in cui le informazioni sono conservate, trasmesse e trattate. Se del caso, tali misure comprendono i seguenti elementi:

   a) restrizioni all'ubicazione geografica;

   b) considerazione di potenziali conflitti di interesse, boicottaggi o sanzioni in relazione ai contraenti;

   c) disposizioni contrattuali per garantire la sicurezza delle informazioni;

   d) cifratura delle informazioni a riposo e in transito;

   e) restrizioni all'accessibilità delle informazioni delle istituzioni e degli organi dell'Unione da parte del personale del contraente;

   f) protezione dei dati personali conformemente alla legislazione applicabile in materia di protezione dei dati.

5. Le istituzioni e gli organi dell'Unione gestiscono i propri CIS nel rispetto dei seguenti principi:

   a) ogni CIS dispone di un proprietario del sistema o di un'autorità operativa per la garanzia di sicurezza delle informazioni responsabile della sua sicurezza;

   b) è eseguita una procedura di gestione del rischio di sicurezza delle informazioni che copra gli aspetti relativi alla sicurezza delle informazioni;

   c) i requisiti di sicurezza e le procedure operative di sicurezza sono formalmente definiti, attuati, verificati e riesaminati;

   d) gli incidenti di sicurezza delle informazioni sono formalmente registrati ed è dato loro seguito, conformemente al regolamento UE [...] che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione.

Capo 4
Informazioni non classificate

Articolo 12

Informazioni ad uso pubblico

1. Le informazioni destinate ad uso pubblico o alla pubblicazione ufficiale o già divulgate, che possono essere condivise senza restrizioni all'interno o all'esterno delle istituzioni e degli organi dell'Unione, sono categorizzate, trattate e conservate come informazioni ad uso pubblico.

2. Le istituzioni e gli organi dell'Unione possono assegnare il contrassegno "PUBLIC USE" alle informazioni di cui al paragrafo 1.

3. Tutte le istituzioni e tutti gli organi dell'Unione garantiscono l'integrità e la disponibilità delle informazioni ad uso pubblico mediante misure adeguate in funzione delle relative esigenze di sicurezza.

Articolo 13

Informazioni normali

1. Le informazioni destinate ad essere utilizzate da un'istituzione o un organo dell'Unione nell'esercizio delle sue funzioni e che non sono né sensibili non classificate né ad uso pubblico sono categorizzate, trattate e conservate come informazioni normali. Tale categoria comprende tutte le informazioni a livello di lavoro normale trattate nell'istituzione o nell'organo dell'Unione in questione.

2. Le informazioni normali possono essere contrassegnate visivamente o con metadati ove necessario per garantirne la protezione, in particolare se condivise al di fuori delle istituzioni e degli organi dell'Unione. In tal caso è utilizzato il contrassegno "EU NORMAL" o "nome o acronimo dell'istituzione o dell'organo dell'Unione NORMAL" (adattato caso per caso).

3. Le istituzioni e gli organi dell'Unione definiscono le misure di protezione standard per le informazioni normali, tenuto conto degli orientamenti del sottogruppo sulle informazioni non classificate e di eventuali rischi specifici connessi ai propri compiti e alle proprie attività.

4. Le informazioni normali sono scambiate al di fuori delle istituzioni e degli organi dell'Unione solo con persone fisiche o giuridiche che hanno una necessità di conoscere.

Articolo 14

Informazioni sensibili non classificate

1. Le istituzioni e gli organi dell'Unione categorizzano, trattano e conservano come informazioni sensibili non classificate tutte le informazioni che non sono classificate ma che essi devono proteggere in virtù di obblighi giuridici o del danno che la loro divulgazione non autorizzata può arrecare ai legittimi interessi privati e pubblici, compresi quelli delle istituzioni e degli organi dell'Unione, degli Stati membri o di persone fisiche.

2. Ogni istituzione e organo dell'Unione identifica le informazioni sensibili non classificate mediante un contrassegno di sicurezza visibile e definisce le corrispondenti istruzioni di trattamento conformemente all'allegato I.

3. Le istituzioni e gli organi dell'Unione proteggono le informazioni sensibili non classificate applicando misure adeguate per quanto riguarda il loro trattamento e la loro conservazione. Tali informazioni possono essere messe a disposizione solo all'interno delle istituzioni e degli organi dell'Unione a persone che hanno una necessità di conoscere ai fini dell'assolvimento dei compiti loro attribuiti.

4. Le informazioni sensibili non classificate sono scambiate al di fuori delle istituzioni e degli organi dell'Unione solo con persone fisiche e giuridiche che hanno una necessità di conoscere, nel rispetto delle istruzioni di trattamento che accompagnano

le informazioni. Tutte le parti coinvolte sono informate delle opportune istruzioni di trattamento.

Articolo 15

Protezione delle informazioni non classificate e interoperabilità

1. Le istituzioni e gli organi dell'Unione stabiliscono procedure per la segnalazione e la gestione di qualsiasi incidente o presunto incidente che possa compromettere la sicurezza delle informazioni non classificate.

2. Ove necessario, le istituzioni e gli organi dell'Unione utilizzano i contrassegni previsti agli articoli 12, 13 e 14. Eccezionalmente, a livello interno e in relazione ai loro omologhi particolari di altre istituzioni e organi dell'Unione o degli Stati membri, possono utilizzare altri contrassegni equivalenti, con l'accordo di tutte le parti. Tale eccezione è notificata al sottogruppo sulle informazioni non classificate di cui all'articolo 7, paragrafo 1, lettera b).

3. Sono stabilite garanzie contrattuali per assicurare la protezione delle informazioni normali e delle informazioni sensibili non classificate trattate dai servizi esternalizzati. Le garanzie sono concepite in modo da assicurare un livello di protezione almeno equivalente a quello previsto dal presente regolamento e comprendono impegni di riservatezza e di non divulgazione che devono essere firmati da tutti i prestatori di servizi pertinenti coinvolti nella fornitura dei sistemi esternalizzati.

Articolo 16

Sottogruppo sulle informazioni non classificate

1. Il sottogruppo sulle informazioni non classificate di cui all'articolo 7, paragrafo 1, lettera b), ha i seguenti ruoli e responsabilità:

   a) razionalizzare le procedure relative al trattamento e alla conservazione delle informazioni non classificate e preparare gli orientamenti pertinenti;

   b) garantire il coordinamento con il sottogruppo sulla garanzia di sicurezza delle informazioni di cui all'articolo 7, paragrafo 1, lettera a), in merito alle questioni relative ai sistemi che trattano e conservano informazioni non classificate;

   c) preparare le istruzioni di trattamento per i diversi livelli di riservatezza delle informazioni non classificate;

   d) assistere le istituzioni e gli organi dell'Unione nello stabilire l'equivalenza tra le loro categorie particolari di informazioni non classificate e quelle previste agli articoli 12, 13 e 14;

   e) agevolare la condivisione delle informazioni non classificate tra le istituzioni e gli organi dell'Unione, fornendo assistenza e orientamenti.

Articolo 17

Trattamento e conservazione delle informazioni sensibili non classificate nei CIS

1. Le istituzioni e gli organi dell'Unione garantiscono che i CIS soddisfino i seguenti requisiti minimi per il trattamento e la conservazione delle informazioni sensibili non classificate:

a) è attuata un'autenticazione forte per l'accesso alle informazioni sensibili non classificate e dette informazioni sono criptate ai fini della trasmissione e conservazione;

b) le chiavi di cifratura utilizzate per la conservazione sono sotto la responsabilità dell'istituzione o dell'organo dell'Unione responsabile del funzionamento del CIS;

c) le informazioni sensibili non classificate sono conservate e trattate nell'Unione;

d) in tutti i contratti di esternalizzazione sono incluse disposizioni contrattuali sulla sicurezza del personale, delle risorse e delle informazioni;

e) sono utilizzati metadati interoperabili per registrare il livello di riservatezza dei documenti elettronici e per facilitare l'automazione delle misure di sicurezza;

f) le istituzioni e gli organi dell'Unione attuano misure volte a prevenire e individuare la fuga di dati per proteggere le informazioni sensibili non classificate;

g) se disponibili, sono utilizzati dispositivi di sicurezza corredati di un certificato europeo di cibersicurezza;

h) attuazione di misure di sicurezza basate sui principi della necessità di conoscere e "zero trust" per ridurre al minimo l'accesso alle informazioni sensibili non classificate da parte dei prestatori di servizi e dei contraenti.

2. Qualsiasi deroga ai requisiti minimi di cui al paragrafo 1 è soggetta all'approvazione dell'adeguato livello di dirigenza dell'istituzione o dell'organo dell'Unione in questione, sulla base di una valutazione del rischio relativa ai rischi giuridici e tecnici per la sicurezza delle informazioni sensibili non classificate.

3. L'autorità di garanzia di sicurezza delle informazioni dell'istituzione o dell'organo dell'Unione in questione può verificare la conformità ai principi di cui al paragrafo 1 in qualsiasi momento durante il ciclo di vita di un CIS.

Capo 5
ICUE

SEZIONE 1
DISPOSIZIONI GENERALI

Articolo 18

Classifiche e contrassegni di sicurezza

1. Le ICUE sono classificate a uno dei seguenti livelli e sono contrassegnate come segue:

a) TRES SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione 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 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 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 o di uno o più Stati membri.

2. Il gruppo di coordinamento adotta documenti di orientamento sulla creazione e la classificazione delle ICUE.

Articolo 19

Idoneità a trattare e conservare ICUE

1. Qualsiasi istituzione e organo dell'Unione può trattare e conservare ICUE se soddisfa le seguenti condizioni:

a) stabilisce norme e procedure conformemente al presente regolamento, garantendo la protezione delle informazioni per un determinato livello di classifica; e

b) è stato sottoposto a una visita di valutazione conformemente all'articolo 53, ed è stato successivamente certificato che può proteggere le ICUE conformemente al presente regolamento e, se del caso, a qualsiasi altra norma e procedura pertinente.

2. Le condizioni di cui al paragrafo 1 si considerano automaticamente soddisfatte dai membri del sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate di cui all'articolo 7, paragrafo 1, lettera e).

Articolo 20

Protezione delle ICUE

1. Il detentore di qualsiasi ICUE è responsabile della loro protezione.

2. Qualora uno Stato membro introduca informazioni classificate recanti un contrassegno di classifica di sicurezza nazionale nelle strutture o nelle reti di un'istituzione o un organo dell'Unione, l'istituzione o l'organo in questione protegge tali informazioni conformemente al corrispondente contrassegno di classifica stabilito nell'accordo tra gli Stati membri dell'Unione europea, riuniti in sede di Consiglio, sulla protezione delle informazioni classificate scambiate nell'interesse dell'Unione europea[29]. La corrispondente tabella di equivalenza figura nell'allegato VI del presente regolamento.

3. Un'aggregazione di ICUE può richiedere un livello di protezione corrispondente a una classifica più elevata di quella dei singoli componenti.

Articolo 21

Procedura di gestione del rischio di sicurezza delle ICUE

1. L'autorità di sicurezza di ogni istituzione e organo dell'Unione approva le misure di sicurezza per proteggere le ICUE durante tutto il loro ciclo di vita conformemente

[29] GU C 202 dell'8.7.2011, pag. 13.

all'esito di una valutazione del rischio effettuata dalla rispettiva istituzione o dal rispettivo organo dell'Unione.

2. Le misure di sicurezza adottate da ogni istituzione e organo dell'Unione sono commisurate al livello di classifica delle informazioni trattate e conservate, alla loro forma e al loro volume, nonché all'ubicazione e alle caratteristiche di protezione delle strutture in cui le ICUE sono trattate e conservate e alla minaccia di attività dolose o criminali valutata a livello locale.

3. Tutte le istituzioni e tutti gli organi dell'Unione stabiliscono:

   a) piani di emergenza per garantire la sicurezza delle ICUE in casi di emergenza;

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

Articolo 22

Violazioni della sicurezza e compromissione di ICUE

1. Un'azione o un'omissione di un'istituzione o un organo dell'Unione o di una persona, che violi il presente regolamento, è da considerarsi una violazione della sicurezza.

2. Le ICUE sono considerate compromesse se, a seguito di una violazione, sono state divulgate, in tutto o in parte, a una o più persone che non sono autorizzate ad accedervi.

3. Qualsiasi compromissione o sospetta compromissione di ICUE è segnalata immediatamente all'autorità di sicurezza dell'istituzione o dell'organo dell'Unione pertinente, che svolge un'indagine di sicurezza e adotta almeno le seguenti misure:

   a) informare l'originatore;

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

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

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

   e) informare le autorità competenti della compromissione accertata o potenziale e delle misure adottate.

SEZIONE 2
SICUREZZA DEL PERSONALE

Articolo 23

Principi di base

1. L'autorità di sicurezza di un'istituzione o un organo dell'Unione può concedere alle persone l'accesso alle ICUE se sono soddisfatte tutte le seguenti condizioni:

   a) le persone hanno una necessità di conoscere;

   b) le persone sono state istruite sulle norme e procedure di sicurezza per la protezione delle ICUE, nonché sulle norme e gli orientamenti di sicurezza pertinenti, e hanno riconosciuto per iscritto le proprie responsabilità in materia di protezione di tali informazioni;

c) per le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore, le persone hanno ottenuto un nulla osta di sicurezza e sono state autorizzate al livello pertinente.

2. Le istituzioni e gli organi dell'Unione tengono conto della lealtà, dell'onestà e dell'affidabilità di una persona, accertate mediante un'indagine di sicurezza condotta dalle autorità competenti dello Stato membro di cui il richiedente è cittadino.

3. Le istituzioni e gli organi dell'Unione possono accettare nulla osta di sicurezza di paesi terzi e organizzazioni internazionali con cui l'Unione abbia concluso un accordo sulla sicurezza delle informazioni.

4. Le istituzioni e gli organi dell'Unione possono gestire le procedure di nulla osta in modo autonomo o stipulare un accordo sul livello dei servizi con la Commissione ai fini del nulla osta di sicurezza.

In caso di conclusione di un accordo sul livello dei servizi, l'autorità di sicurezza della Commissione è il punto di contatto tra gli uffici di sicurezza dell'istituzione o dell'organo dell'Unione in questione e le competenti autorità nazionali degli Stati membri per quanto riguarda i nulla osta di sicurezza.

5. L'autorità di sicurezza di ogni istituzione e organo dell'Unione conserva una registrazione dei nulla osta di sicurezza, delle informative, delle attestazioni scritte e delle autorizzazioni di accesso alle ICUE.

6. Le istituzioni e gli organi dell'Unione che concludono un accordo sul livello dei servizi con la Commissione mettono le pertinenti registrazioni a disposizione dell'autorità di sicurezza della Commissione per quanto riguarda almeno il livello di ICUE cui può accedere la persona in questione, la data di rilascio dell'autorizzazione di accesso alle ICUE e il relativo periodo di validità. Tali registrazioni sono accessibili alle altre istituzioni e organi dell'Unione che hanno un accordo sul livello dei servizi, ove giustificato.

Articolo 24

Autorizzazione di accesso alle ICUE

1. Ogni istituzione e organo dell'Unione individua al proprio interno le posizioni che richiedono l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore che consentono al detentore di assolvere le proprie funzioni.

2. Laddove una persona necessiti di essere autorizzata ad accedere a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, l'istituzione o l'organo in questione informa l'autorità di sicurezza competente, che procede alle formalità di cui al punto 1 dell'allegato II.

3. L'autorità di sicurezza di ogni istituzione e organo dell'Unione è responsabile del rilascio, della sospensione, della revoca e del rinnovo delle autorizzazioni di accesso alle ICUE per il relativo personale.

4. In circostanze eccezionali, laddove sia debitamente giustificato nell'interesse del servizio e in attesa dell'esito dell'intera indagine di sicurezza, l'autorità di sicurezza di un'istituzione o un organo dell'Unione può rilasciare un'autorizzazione temporanea per accedere alle ICUE per una posizione specifica, fatte salve le disposizioni

relative al rinnovo delle autorizzazioni di accesso alle ICUE e previa verifica dell'autorità di sicurezza nazionale pertinente.

5. Le istituzioni e gli organi dell'Unione seguono le procedure di gestione delle autorizzazioni di accesso alle ICUE di cui all'allegato II.

Articolo 25

Riconoscimento delle autorizzazioni di accesso alle ICUE

1. Un'autorizzazione di accesso alle ICUE fino al livello specificato è valida in qualsiasi istituzione o organo dell'Unione cui la persona è assegnata.

2. Le istituzioni e gli organi dell'Unione accettano le autorizzazioni di accesso alle ICUE rilasciate da altre istituzioni o organi dell'Unione.

3. Qualora il titolare di un'autorizzazione di accesso alle ICUE sia assunto presso un'altra istituzione o un altro organo dell'Unione, tale istituzione o organo dell'Unione notifica all'NSA pertinente il cambiamento di datore di lavoro tramite l'autorità di sicurezza competente.

Articolo 26

Informativa sulle ICUE

1. L'autorità di sicurezza di un'istituzione o un organo dell'Unione informa tutte le persone che necessitano di accedere alle ICUE in merito a qualsiasi minaccia alla sicurezza e all'obbligo di segnalare qualsiasi attività sospetta. L'informativa ha luogo prima della concessione dell'accesso alle ICUE e successivamente almeno ogni cinque anni.

2. Dopo aver ricevuto l'informativa di cui al paragrafo 1, tutte le persone interessate riconoscono per iscritto di aver compreso gli obblighi di protezione delle ICUE e le eventuali conseguenze se le ICUE risultano compromesse.

3. L'informativa di cui al paragrafo 1 comprende le seguenti informazioni:

   a) ogni persona responsabile di una violazione delle norme di sicurezza contenute nel presente regolamento è passibile di azione disciplinare conformemente alle disposizioni legislative e regolamentari applicabili;

   b) ogni persona responsabile della compromissione o della perdita di ICUE è passibile di sanzioni disciplinari o azioni legali conformemente alle disposizioni legislative, normative e regolamentari applicabili.

4. Se le persone cui è stata rilasciata un'autorizzazione di accesso alle ICUE non necessitano più dell'accesso, le istituzioni e gli organi dell'Unione provvedono affinché tali persone siano informate dell'obbligo di continuare a proteggere le ICUE e, se del caso, riconoscano per iscritto quest'obbligo.

5. Il compito di creare e gestire le informative sulle ICUE può essere condiviso tra le istituzioni e gli organi dell'Unione, purché siano presi in considerazione i loro requisiti specifici.

SEZIONE 3
SICUREZZA MATERIALE

Articolo 27

Principi di base

1. Ogni istituzione e organo dell'Unione stabilisce le misure di sicurezza materiale adeguate ai propri siti, conformemente all'allegato III e al principio di difesa in profondità, sulla base di una valutazione del rischio effettuata dalla propria autorità di sicurezza. Le misure perseguono i seguenti obiettivi:

   a) impedire l'accesso alle ICUE o l'ingresso con la forza da parte di intrusi;

   b) scoraggiare, ostacolare e scoprire azioni non autorizzate e rispondere quanto prima agli incidenti di sicurezza;

   c) consentire la segregazione del personale per quanto riguarda l'accesso alle ICUE sulla base del principio della necessità di conoscere e, in caso, del nulla osta di sicurezza;

2. Le istituzioni e gli organi dell'Unione attuano misure di sicurezza materiale per tutti i siti in cui le ICUE sono discusse, conservate o trattate, comprese le zone che contengono i sistemi di comunicazione e informazione definiti alla sezione 5 del presente capo.

3. Per la protezione materiale delle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono utilizzate solo le attrezzature di sicurezza approvate dall'autorità di sicurezza di un'istituzione o un organo dell'Unione.

4. Le istituzioni e gli organi dell'Unione possono condividere le zone protette di cui all'allegato III per il trattamento e la conservazione delle ICUE, previa conclusione di un accordo.

Articolo 28

Sottogruppo sulla sicurezza materiale

1. Il sottogruppo sulla sicurezza materiale di cui all'articolo 7, paragrafo 1, lettera c), ha i seguenti ruoli e responsabilità:

   a) elaborare documenti di orientamento in materia di sicurezza fisica;

   b) definire i criteri di sicurezza generali per l'acquisto di attrezzature, quali contenitori di sicurezza, macchine sminuzzatrici, serrature di porte, sistemi elettronici di controllo dell'accesso, sistemi di rilevamento delle intrusioni, sistemi d'allarme, per la protezione materiale delle ICUE;

   c) assistere le istituzioni e gli organi dell'Unione nella definizione delle misure di sicurezza adeguate ai loro siti;

   d) proporre misure compensative per la protezione delle ICUE quando le ICUE sono trattate al di fuori delle zone oggetto di protezione materiale di un'istituzione o un organo dell'Unione.

Articolo 29

Protezione materiale delle ICUE

1. Per garantire la protezione materiale delle ICUE, le istituzioni e gli organi dell'Unione stabiliscono le seguenti zone oggetto di protezione materiale:

   a) le zone amministrative di cui all'allegato III;

   b) ove opportuno, le zone protette, comprese le zone protette di categoria I e di categoria II e le zone protette tecnicamente, di cui all'allegato III.

2. L'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione effettua un'ispezione interna per verificare se una zona soddisfa le condizioni di cui all'allegato III per costituire una zona amministrativa o una zona protetta. Se il rapporto di ispezione indica che le condizioni sono soddisfatte, l'autorità di sicurezza può rilasciare un accreditamento della zona protetta a proteggere le ICUE fino al livello dichiarato per un periodo non superiore a cinque anni.

   L'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione è responsabile dello svolgimento della procedura di riaccreditamento delle zone protette prima della scadenza dell'accreditamento o in caso di attuazione di modifiche all'interno della zona accreditata.

3. Ogni istituzione e organo dell'Unione adotta le procedure di gestione delle chiavi e delle combinazioni per gli uffici, le stanze, le camere blindate e i contenitori di sicurezza in cui sono conservate informazioni di livello CONFIDENTIEL UE/EU-CONFIDENTIAL e superiore.

4. L'autorità di sicurezza può autorizzare ispezioni all'entrata e all'uscita per scoraggiare e individuare l'introduzione non autorizzata di materiale o la sottrazione non autorizzata di ICUE dai siti.

5. Le istituzioni e gli organi dell'Unione stabiliscono le misure per la protezione materiale delle ICUE conformemente all'allegato III.

SEZIONE 4
GESTIONE DELLE ICUE

Articolo 30

Principi di base

1. Le istituzioni e gli organi dell'Unione registrano, archiviano, conservano e da ultimo eliminano, campionano o trasferiscono i propri documenti ICUE agli archivi pertinenti conformemente alla politica e alle norme di conservazione specifiche dei fascicoli di ogni istituzione e organo dell'Unione.

2. Ogni istituzione e organo dell'Unione originatore di ICUE determina la classifica di sicurezza delle informazioni al momento della loro creazione e conformemente all'articolo 18, paragrafo 1.

3. Le istituzioni e gli organi dell'Unione comunicano chiaramente ai destinatari il livello di classifica mediante un contrassegno di classifica o un annuncio, se le informazioni sono fornite oralmente.

4. Le misure di sicurezza applicabili al documento originale si applicano ai progetti, alle copie e alle traduzioni.

5. Le istituzioni e gli organi dell'Unione stabiliscono le misure per la gestione delle ICUE conformemente all'allegato IV.

Articolo 31

Creazione di ICUE

2. Le istituzioni e gli organi dell'Unione sotto la cui autorità sono create ICUE assicurano che siano soddisfatti i seguenti requisiti:

a) ciascuna pagina è contrassegnata chiaramente con il livello di classifica;

b) ciascuna pagina è numerata;

c) il documento reca un numero di riferimento, se del caso un numero di registrazione e un oggetto che non è in sé un'ICUE, a meno che non sia contrassegnato come tale;

d) il documento riporta la data in cui è stato creato;

e) tutti gli allegati e il materiale accluso sono elencati, ove possibile, sulla prima pagina;

f) i documenti classificati di livello SECRET UE/EU SECRET o superiore che debbano essere distribuiti in più copie recano un numero di copia su ciascuna pagina. Le copie elettroniche distribuite al di fuori del sistema detentore recano un identificativo univoco basato su una firma elettronica.

Articolo 32

Controllo dell'originatore

1. L'istituzione o l'organo dell'Unione sotto la cui autorità è creato un documento ICUE esercita il controllo dell'originatore su tale documento. L'originatore determina il livello di classifica del documento ed è responsabile della sua diffusione iniziale. Fatto salvo il regolamento (CE) n. 1049/2001, il previo consenso scritto dell'originatore è necessario prima che le informazioni siano:

a) declassificate o declassate;

b) utilizzate a fini diversi da quelli stabiliti dall'originatore;

c) trasmesse a qualsiasi entità esterna all'istituzione o all'organo dell'Unione che detiene le informazioni, compresi un paese terzo o un'organizzazione internazionale, un'altra istituzione o un altro organo dell'Unione, gli Stati membri, un contraente o potenziale contraente, un beneficiario o potenziale beneficiario;

d) copiate e tradotte in caso di livello TRES SECRET-UE/EU-TOP SECRET.

2. Se non è possibile individuare l'originatore di un documento ICUE, l'istituzione o l'organo dell'Unione che detiene tali informazioni classificate esercita il controllo dell'originatore.

3. Gli originatori di qualsiasi documento ICUE tengono un registro di tutte le fonti classificate utilizzate per produrre documenti classificati, compresi i dettagli delle fonti provenienti dagli Stati membri, da organizzazioni internazionali o da paesi terzi. Se del caso, le informazioni classificate aggregate sono contrassegnate in modo da preservare l'identificazione degli originatori delle fonti classificate utilizzate.

Articolo 33

Contrassegni di classifica

1. Se del caso, oltre a uno dei contrassegni di classifica di sicurezza, i documenti ICUE possono recare altri contrassegni, quali contrassegni di distribuzione o di divulgabilità o contrassegni per indicare l'originatore.

2. Parti diverse di un documento ICUE possono richiedere classifiche differenti e sono contrassegnate di conseguenza. Il livello di classifica generale di un documento o file corrisponde come minimo a quello del suo componente di livello più elevato.

3. 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.

Articolo 34

Sistema di registrazione delle ICUE

1. Tutte le istituzioni e tutti gli organi dell'Unione che trattano e conservano informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIEL o superiore istituiscono uno o più uffici di registrazione delle ICUE per garantirne la registrazione a fini di sicurezza quando entrano o lasciano un'istituzione o un organo dell'Unione.

2. Tutti gli uffici di registrazione delle ICUE sono istituiti in zone protette di cui all'allegato III.

3. Le istituzioni e gli organi dell'Unione assegnano un funzionario responsabile del controllo delle registrazioni ("RCO") alla gestione di ciascun ufficio di registrazione delle ICUE. L'RCO deve essere munito di apposito nulla osta di sicurezza ed essere autorizzato conformemente all'articolo 24. Le istituzioni e gli organi dell'Unione assicurano una formazione adeguata per il proprio RCO.

Articolo 35

Declassamento e declassificazione

1. Le informazioni restano classificate solo finché necessitano di protezione. Le ICUE che non necessitano più della classifica originaria sono declassate a un livello inferiore. Le ICUE che non necessitano più di essere considerate classificate sono declassificate.

2. Al momento della creazione delle ICUE l'originatore indica, laddove possibile e in particolare per le informazioni classificate RESTREINT UE/EU RESTRICTED, se le ICUE possono essere declassate o declassificate a una certa data o in seguito a un dato evento.

3. L'istituzione o l'organo dell'Unione di origine è responsabile della decisione in merito al declassamento o alla declassificazione di un documento ICUE. Essa o esso esamina le informazioni e valuta i rischi periodicamente, almeno ogni cinque anni, al fine di determinare se il livello di classifica iniziale sia ancora giustificato.

4. Le istituzioni e gli organi dell'Unione che detengono un documento ICUE di cui non sono l'originatore non lo declassano o declassificano, né modificano o rimuovono i

contrassegni di cui all'articolo 18, paragrafo 1, senza il previo consenso scritto dell'originatore.

5. Le istituzioni e gli organi dell'Unione possono declassare o declassificare parzialmente le ICUE da essi create. In tali casi è prodotto un estratto declassato o declassificato.

6. Le istituzioni e gli organi dell'Unione informano l'organizzazione destinataria delle ICUE del declassamento o della declassificazione.

Articolo 36

Contrassegni sui documenti declassati o declassificati

1. Qualora decidano di declassificare un documento ICUE, le istituzioni e gli organi dell'Unione considerano se il documento debba recare il contrassegno per la distribuzione delle informazioni sensibili non classificate.

2. Il contrassegno originale di classifica in alto e in basso di ogni pagina è barrato in modo visibile utilizzando la funzione "barrato" per i formati elettronici, o manualmente per i documenti stampati. Il contrassegno originale di classifica non è rimosso.

3. La prima pagina o la pagina di copertina è timbrata come declassata o declassificata e compilata con i dati dell'autorità responsabile del declassamento o della declassificazione e la relativa data. Il declassamento o la declassificazione di documenti ICUE elettronici è attestato da una firma elettronica sotto l'autorità dell'originatore.

Articolo 37

Distruzione e cancellazione delle ICUE

1. Le istituzioni e gli organi dell'Unione riesaminano le ICUE, sia su carta che nei CIS, almeno ogni cinque anni per stabilire se debbano essere distrutte o cancellate. Qualora le ICUE siano distrutte o cancellate, impartiscono istruzioni a chiunque le abbia precedentemente ricevute.

2. Le istituzioni e gli organi dell'Unione possono distruggere duplicati di ICUE che non sono più necessari, tenuto conto delle pertinenti norme sulla gestione dei documenti per gli originali.

3. Le istituzioni e gli organi dell'Unione distruggono le copie cartacee di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore solo tramite il loro funzionario responsabile del controllo delle registrazioni. L'RCO aggiorna di conseguenza i repertori e gli altri dati relativi alla registrazione, conservando i metadati essenziali del documento distrutto.

   I documenti classificati di livello SECRET UE/EU SECRET o superiore sono distrutti solo dal funzionario responsabile del controllo delle registrazioni in presenza di un testimone che possiede un nulla osta di sicurezza almeno fino al livello di classifica del documento da distruggere.

4. L'RCO e, se del caso, il testimone firmano un certificato di distruzione che è archiviato presso l'ufficio di registrazione. Il certificato è conservato per almeno cinque anni nel caso di informazioni classificate CONFIDENTIEL UE/EU

CONFIDENTIAL o SECRET-UE/EU-SECRET e per almeno dieci anni nel caso di informazioni classificate TRES SECRET-UE/EU-TOP SECRET.

Articolo 38

Evacuazione e distruzione delle ICUE in casi di emergenza

1. Ogni istituzione e organo dell'Unione elabora piani di evacuazione e di distruzione di emergenza sulla base delle condizioni locali per la salvaguardia delle ICUE che presentano un rischio significativo di cadere in mano a persone non autorizzate.

   I dettagli operativi dei piani di evacuazione e di distruzione di emergenza sono classificati come RESTREINT UE/EU RESTRICTED.

2. In caso di emergenza, se c'è un rischio imminente di divulgazione non autorizzata di ICUE, le istituzioni e gli organi dell'Unione evacuano le ICUE.

   Se l'evacuazione non è possibile le ICUE sono distrutte in modo tale da non poter essere ricostruite in tutto o in parte.

3. L'originatore e l'ufficio di registrazione d'origine sono informati dell'evacuazione o della distruzione d'emergenza delle ICUE registrate.

4. Se sono stati attivati piani di emergenza, è data priorità all'evacuazione o alla distruzione dei livelli superiori di ICUE, compresa l'attrezzatura di cifratura.

Articolo 39

Archiviazione

1. Le istituzioni e gli organi dell'Unione decidono in merito all'archiviazione delle ICUE e alle misure pratiche corrispondenti conformemente alla propria politica di gestione dei documenti.

2. I documenti ICUE non sono trasferiti agli archivi storici dell'Unione europea.

SEZIONE 5
PROTEZIONE DELLE ICUE NEI SISTEMI DI COMUNICAZIONE E INFORMAZIONE (CIS)

Articolo 40

Sottogruppo sull'accreditamento dei sistemi di comunicazione e informazione che trattano e conservano ICUE

Il sottogruppo sull'accreditamento dei sistemi di comunicazione e informazione che trattano e conservano ICUE di cui all'articolo 7, paragrafo 1, lettera d), ha i seguenti ruoli e responsabilità:

a) assistere le istituzioni e gli organismi dell'Unione nelle procedure di accreditamento;

b) raccomandare una norma di accreditamento che tutte le istituzioni e tutti gli organi dell'Unione devono seguire;

c) diffondere e condividere le migliori pratiche e gli orientamenti in materia di accreditamento dei CIS.

Articolo 41

Sistemi di comunicazione e informazione

Le istituzioni e gli organi dell'Unione soddisfano i seguenti requisiti in relazione ai CIS che trattano e conservano ICUE:

a) il proprietario del sistema o l'autorità operativa per la garanzia di sicurezza delle informazioni consulta l'autorità di accreditamento di sicurezza prima di sviluppare, acquisire o consentire a un CIS di trattare e conservare ICUE, al fine di determinare i requisiti per l'accreditamento;

b) i principi di sicurezza fondamentali per la progettazione dei CIS che trattano e conservano ICUE si applicano all'inizio del progetto, nell'ambito della procedura di gestione del rischio di sicurezza delle informazioni e tenuto conto dei principi della necessità di conoscere, della funzionalità minima, della difesa in profondità, del privilegio minimo, della separazione delle funzioni e del doppio controllo;

c) i componenti relativi alla conservazione, al trattamento centrale e alla gestione della rete di un CIS che tratta e conserva ICUE sono installati in una zona protetta di cui all'allegato III;

d) attuano "misure di sicurezza TEMPEST" commisurate al rischio di sfruttamento e al livello di classifica delle informazioni;

e) tutto il personale coinvolto nel funzionamento di un CIS che tratta e conserva ICUE informa l'autorità di sicurezza e il pertinente proprietario del sistema o la pertinente autorità operativa per la garanzia di sicurezza delle informazioni in merito a ogni potenziale lacuna, incidente, violazione della sicurezza o compromissione del sistema che possa avere conseguenze sulla protezione del CIS o delle ICUE in esso contenute;

f) se del caso, l'autorità di sicurezza informa le autorità di sicurezza di ogni altra istituzione e altro organo dell'Unione interessati in merito a potenziali lacune o incidenti di sicurezza che potrebbero avere conseguenze sui loro CIS che trattano e conservano ICUE.

Articolo 42

Prodotti crittografici

1. Per la trasmissione e la conservazione di ICUE mediante mezzi elettronici sono utilizzati prodotti crittografici approvati. L'elenco dei prodotti crittografici approvati è mantenuto dal Consiglio, sulla base del contributo delle autorità di sicurezza nazionali.

2. Se nell'elenco di cui al paragrafo 1 non figura alcun prodotto idoneo allo scopo previsto, l'autorità di approvazione degli apparati crittografici dell'istituzione o dell'organo dell'Unione in questione chiede un'approvazione temporanea al Consiglio. Ove possibile, è selezionato un prodotto crittografico approvato dall'autorità di sicurezza nazionale di uno Stato membro.

   Il Consiglio adotta le misure necessarie per garantire che un prodotto idoneo sia aggiunto all'elenco.

3. L'approvazione di un prodotto crittografico è valida per un massimo di cinque anni ed è successivamente riesaminata su base annuale.

4. Il Consiglio rimuove dall'elenco dei prodotti crittografici approvati qualsiasi prodotto crittografico la cui approvazione nazionale sia stata revocata o sia scaduta.

5. Ogni anno il gruppo di coordinamento informa il Consiglio in merito ai prodotti crittografici per i quali raccomanda una valutazione da parte di un'autorità di approvazione degli apparati crittografici di uno Stato membro sulla base di un'indagine condotta presso le istituzioni e gli organi dell'Unione.

Articolo 43

Accreditamento dei CIS che trattano e conservano ICUE

1. Accreditando i CIS che trattano e conservano ICUE, le istituzioni e gli organi dell'Unione confermano 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 al presente regolamento.

2. Il proprietario del CIS o l'autorità operativa per la garanzia di sicurezza delle informazioni è responsabile della preparazione dei fascicoli e della documentazione di accreditamento, compresi i manuali per i diversi tipi di utenti.

3. L'autorità di accreditamento di sicurezza di ogni istituzione e organo dell'Unione è responsabile di stabilire una procedura di accreditamento con condizioni chiare che devono essere approvate, per tutti i CIS sotto la loro autorità.

4. Qualora un CIS che tratta e conserva ICUE coinvolga sia istituzioni e organi dell'Unione che autorità di sicurezza nazionali, le istituzioni e gli organi dell'Unione interessati istituiscono, mediante ulteriori norme di attuazione adottate a norma dell'articolo 8, paragrafo 2, un comitato di accreditamento di sicurezza comune incaricato dell'accreditamento del sistema. Tale comitato è composto dai rappresentanti dell'autorità di accreditamento di sicurezza delle parti coinvolte ed è presieduto dall'autorità di accreditamento di sicurezza dell'istituzione o dell'organo dell'Unione proprietario del CIS.

Articolo 44

Procedura di accreditamento di CIS che trattano e conservano ICUE

1. Tutti i CIS che trattano e conservano ICUE sono soggetti a una procedura di accreditamento basata sui principi della garanzia di sicurezza delle informazioni, il cui livello di dettaglio è commisurato al livello di protezione richiesto.

2. La procedura di accreditamento dà luogo a una dichiarazione di accreditamento che determina il livello di classifica più elevato delle informazioni che può essere trattato e conservato in un CIS nonché i termini e le condizioni ivi associati. La dichiarazione di accreditamento si basa sulla convalida formale della valutazione del rischio e delle misure di sicurezza attuate per il CIS pertinente, fornendo la garanzia di quanto segue:

   a) la procedura di gestione del rischio di sicurezza delle informazioni è stata effettuata in modo adeguato;

   b) il proprietario del sistema o il titolare del rischio ha accettato consapevolmente il rischio residuo;

   c) è stato raggiunto un livello sufficiente di protezione del CIS, e delle ICUE in esso trattate e conservate, conformemente al presente regolamento.

3. L'autorità di accreditamento di sicurezza di un'istituzione o un organo dell'Unione convalida formalmente la dichiarazione di accreditamento. A convalida effettuata, l'autorità di accreditamento di sicurezza rilascia un'approvazione a operare che determina il livello di classifica più elevato delle ICUE che può essere trattato nel CIS nonché i termini e le condizioni associati al funzionamento. L'approvazione è rilasciata per un periodo specifico. Qualora una o più misure di sicurezza richieste non siano attuate ma ciò non abbia un impatto significativo sulla sicurezza complessiva, può essere rilasciata un'approvazione a operare temporanea, specificante i punti cui portare rimedio.

4. In qualsiasi momento del ciclo di vita di un CIS, l'autorità di accreditamento di sicurezza dell'istituzione o dell'organo dell'Unione in questione può intraprendere le seguenti azioni:

   a) applicare una procedura di accreditamento;

   b) effettuare audit o ispezioni del CIS;

   c) qualora non siano più soddisfatte le condizioni di funzionamento, ad esempio quando un incidente di sicurezza ha rivelato una vulnerabilità significativa del CIS, chiedere la definizione e l'attuazione effettiva di un piano di miglioramento della sicurezza entro tempi ben definiti, arrivando a ritirare l'autorizzazione al funzionamento del CIS fino a quando le condizioni di funzionamento non siano soddisfatte.

5. Durante il periodo di validità dell'approvazione a operare il proprietario del sistema o l'autorità operativa per la garanzia di sicurezza delle informazioni presenta annualmente all'autorità di accreditamento di sicurezza una relazione formale, comprensiva di una sintesi degli eventuali incidenti, modifiche e fattori di rischio significativi.

Articolo 45

Situazioni di emergenza

1. Le istituzioni e gli organi dell'Unione possono applicare procedure specifiche per la trasmissione o la conservazione di ICUE classificate in casi di emergenza, come in situazioni di crisi, conflitti, guerre imminenti o già in corso o in circostanze operative eccezionali, previa approvazione della propria autorità di approvazione degli apparati crittografici.

2. Nelle circostanze di cui al paragrafo 1 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, nel rispetto delle seguenti condizioni:

   a) il mittente o il destinatario non ha l'attrezzatura di cifratura necessaria;

   b) il materiale classificato non può essere trasmesso in tempo utile con altri mezzi.

3. Le informazioni classificate trasmesse conformemente al paragrafo 2 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, con altri mezzi, del livello di classifica.

4. Un successivo rapporto sulla trasmissione delle ICUE nelle circostanze di cui al paragrafo 1 è presentato all'autorità di sicurezza pertinente.

SEZIONE 6
SICUREZZA INDUSTRIALE

Articolo 46

Principi di base

1. Ogni istituzione od organo dell'Unione, in quanto autorità contraente o che eroga la sovvenzione, nell'aggiudicare un contratto o una convezione di sovvenzione classificati, assicura che le norme minime sulla sicurezza industriale di cui alla presente sezione e le condizioni per la protezione delle ICUE nei contratti e nelle convenzioni di sovvenzione classificati di cui all'allegato V siano menzionate o integrate nel contratto o nella convenzione di sovvenzione e siano rispettate.

2. Per "sicurezza industriale" si intende l'applicazione di misure che assicurino la protezione delle ICUE da parte delle seguenti persone o entità:

   a) in regime di gestione diretta[30], nell'ambito di contratti classificati, da parte di:

      i) candidati od offerenti attraverso la procedura di appalto e aggiudicazione;

      ii) contraenti o subcontraenti lungo tutto il ciclo di vita dei contratti classificati;

   b) in regime di gestione diretta[31], nell'ambito di convenzioni di sovvenzione classificate, da parte di:

      i) richiedenti durante le procedure di concessione di una sovvenzione;

      ii) beneficiari o subcontraenti lungo tutto il ciclo di vita delle convenzioni di sovvenzione classificate.

   c) in regime di gestione indiretta, nel quadro di accordi quadro relativi ai partenariati finanziari ("FFPA") e dei relativi accordi di contributo, da parte delle entità che ricevono l'incarico durante l'intero ciclo di vita di tali accordi.

3. In quanto entità che conferisce l'incarico, l'istituzione o l'organo dell'Unione descrive i requisiti di sicurezza specifici per l'entità incaricata nel capo sulla sicurezza dell'FFPA e dei relativi accordi di contributo. Tali requisiti si basano sui principi e sulle disposizioni di sicurezza previsti dal presente regolamento in relazione ai contratti e alle convenzioni di sovvenzione classificati, che si applicano mutatis mutandis.

4. I contratti e le convenzioni di sovvenzione classificati non contemplano le informazioni classificate di livello TRES SECRET UE/EU TOP SECRET.

5. Le disposizioni del presente capo relative ai contratti o contraenti classificati, o alle convenzioni di sovvenzione o beneficiari classificati, si applicano anche ai subcontratti o subcontraenti classificati nel significato di, rispettivamente, contratti o sovvenzioni classificati.

6. Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, cooperano strettamente con le autorità di sicurezza o altre autorità

30 Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio.

31 Ibidem.

competenti del paese nel cui territorio ha sede la parte contrattuale o il destinatario della sovvenzione, nonché con le autorità di sicurezza o altre autorità competenti dell'organizzazione internazionale aggiudicataria o beneficiaria della sovvenzione.

7. Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, comunicano con le autorità di sicurezza o altre autorità competenti tramite le proprie autorità di sicurezza.

8. Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, informano le autorità di cui al paragrafo 6, tramite la propria autorità di sicurezza, ogni volta che sia stato firmato un contratto o una convenzione di sovvenzione classificati.

   La notifica comprende i dati pertinenti, quali il nome del contraente o dei beneficiari, la durata del contratto o della convenzione di sovvenzione classificati e il livello massimo di classifica.

   Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, informano le autorità di cui al paragrafo 6 ogni volta che sia stato estinto anticipatamente un contratto o una convenzione di sovvenzione classificati.

9. Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, possono assegnare contratti classificati o parti classificate di convenzioni di sovvenzione solo a entità aventi sede in quei paesi terzi o istituite da quelle organizzazioni internazionali che hanno concluso un accordo sulla sicurezza delle informazioni con l'Unione. Se le ICUE in questione contengono dati personali, il trasferimento di questi ultimi verso un paese terzo o un'organizzazione internazionale è effettuato conformemente al regolamento (UE) 2018/1725.

Articolo 47

Elementi di sicurezza in un contratto o in una convenzione di sovvenzione classificati

1. I contratti o le convenzioni di sovvenzione classificati comprendono i seguenti elementi di sicurezza:

   a) guida alle classifiche di sicurezza;

   b) lettera sugli aspetti di sicurezza.

2. I contratti o le convenzioni di sovvenzione classificati possono includere un'istruzione di sicurezza del programma o progetto.

Articolo 48

Guida alle classifiche di sicurezza

1. Prima di firmare un contratto o una convenzione di sovvenzione classificati, l'istituzione o l'organo dell'Unione, in quanto autorità contraente o che eroga la sovvenzione, determina la classifica di sicurezza di tutte le informazioni che devono essere create dai contraenti o dai beneficiari o dai loro subcontraenti. A tal fine, mette a punto una guida alle classifiche di sicurezza da utilizzare per l'esecuzione del contratto o della convenzione di sovvenzione classificati.

2. La guida alle classifiche di sicurezza può essere modificata per tutta la durata del programma o progetto, di cui all'articolo 50, del contratto o della convenzione di sovvenzione e gli elementi informativi possono essere riclassificati o declassati.

3. Per stabilire la classifica di sicurezza dei vari elementi di un contratto o una convenzione di sovvenzione classificati si applicano i principi seguenti:

a) nel redigere la guida alle classifiche di sicurezza, l'istituzione o l'organo dell'Unione, in quanto autorità contraente o che eroga la sovvenzione, 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 o la convenzione di sovvenzione classificati;

b) il livello generale di classifica del contratto o della convenzione di sovvenzione classificati non è inferiore alla classifica più elevata di uno dei suoi elementi;

c) se del caso, l'istituzione o l'organo dell'Unione in questione, in quanto autorità contraente o che eroga la sovvenzione, si mette in contatto, tramite la propria autorità di sicurezza, con le autorità di sicurezza o altre autorità competenti del paese interessato in caso di eventuali modifiche della guida alle classifiche di sicurezza.

Articolo 49

Lettera sugli aspetti di sicurezza

1. Ogni istituzione od organo dell'Unione, in quanto autorità contraente o che eroga la sovvenzione, descrive i requisiti di sicurezza specifici del contratto o della convenzione di sovvenzione classificati in una lettera sugli aspetti di sicurezza. Tale lettera contiene la guida alle classifiche di sicurezza ed è parte integrante del contratto, convenzione di sovvenzione o subcontratto classificati.

2. La lettera sugli aspetti di sicurezza contiene disposizioni che impongono al contraente o beneficiario e ai suoi subcontraenti di rispettare le disposizioni del presente regolamento e le eventuali ulteriori norme di attuazione, adottate a norma dell'articolo 8, paragrafo 2, in materia di sicurezza industriale. La lettera sugli aspetti di sicurezza indica chiaramente che l'inosservanza di tali disposizioni può essere motivo sufficiente di estinzione del contratto o della convenzione di sovvenzione classificati.

Articolo 50

Istruzione di sicurezza del programma o progetto

1. Le istituzioni e gli organi dell'Unione, in quanto autorità contraenti o che erogano la sovvenzione, possono elaborare un'istruzione di sicurezza del programma o progetto, in stretta cooperazione con le rispettive autorità di sicurezza, in particolare per i programmi e i progetti caratterizzati da portata, entità o complessità considerevoli o dalla molteplicità o la diversità dei contraenti, dei beneficiari nonché degli altri partner e parti interessate coinvolti.

2. L'autorità di sicurezza di ogni istituzione od organo dell'Unione, in quanto autorità contraente o che eroga la sovvenzione, chiede un parere sull'istruzione di sicurezza del programma o progetto specifica ai pertinenti organi consultivi per la sicurezza degli Stati membri, costituiti dalle rispettive autorità di sicurezza nazionali e/o dalle autorità di sicurezza designate.

Se un'istituzione o un organo dell'Unione non dispone di tale organo consultivo, l'istruzione di sicurezza del programma o progetto è presentata al comitato per la sicurezza delle informazioni di cui all'articolo 6, paragrafo 8.

SEZIONE 7
CONDIVISIONE DI ICUE E SCAMBIO DI INFORMAZIONI CLASSIFICATE

Articolo 51

Principi di base

1. Tutte le istituzioni e tutti gli organi dell'Unione possono condividere ICUE con altre istituzioni o altri organi dell'Unione alle condizioni di cui all'articolo 54.

2. Le istituzioni e gli organi dell'Unione possono condividere ICUE con gli Stati membri e la Comunità europea dell'energia atomica purché questi proteggano tali informazioni conformemente al corrispondente contrassegno di classifica stabilito nell'accordo tra gli Stati membri dell'Unione, riuniti in sede di Consiglio, sulla protezione delle informazioni classificate scambiate nell'interesse dell'Unione e alla corrispondente tabella di cui all'allegato VI del presente regolamento.

3. Le istituzioni e gli organi dell'Unione scambiano informazioni classificate solo con i paesi terzi e le organizzazioni internazionali con cui sono stati conclusi accordi sulla sicurezza delle informazioni o intese amministrative conformemente agli articoli 55 e 56.

   Tali accordi e intese contengono disposizioni volte a garantire che i paesi terzi o le organizzazioni internazionali che ricevono le ICUE assicurino un livello di protezione commisurato al livello di classifica e conforme a norme minime non meno rigorose di quelle previste nel presente regolamento.

4. In assenza di un accordo sulla sicurezza delle informazioni o di un'intesa amministrativa, un'istituzione o un organo dell'Unione può, in circostanze eccezionali, comunicare ICUE a un'altra istituzione o un altro organo dell'Unione, a un paese terzo o a un'organizzazione internazionale conformemente all'articolo 58.

5. Le istituzioni e gli organi dell'Unione designano gli uffici di registrazione che fungono da principali punti di ingresso e di uscita per le ICUE condivise con altre istituzioni o altri organi dell'Unione o per le informazioni classificate scambiate con paesi terzi e organizzazioni internazionali.

Articolo 52

Sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate

1. Il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate di cui all'articolo 7, paragrafo 1, lettera e), ha i seguenti ruoli e responsabilità:

   a) organizzare visite di valutazione presso le istituzioni e gli organi dell'Unione, i paesi terzi e le organizzazioni internazionali e adottare il programma annuale delle visite;

   b) preparare ed effettuare le visite di valutazione;

   c) redigere una relazione sugli esiti delle visite di cui alla lettera a)

   tranne nei casi di cui all'articolo 56, paragrafo 2.

2. Il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate è composto da rappresentanti della Commissione, del Consiglio e del servizio europeo per l'azione esterna e delibera per consenso.

Articolo 53

Visite di valutazione relative alla condivisione di ICUE

1. Il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate effettua le visite di valutazione in piena cooperazione con i funzionari dell'istituzione o dell'organo dell'Unione visitato. Può chiedere assistenza all'NSA nel cui territorio si trova l'istituzione o l'organo dell'Unione.

2. Le visite di valutazione presso le istituzioni e gli organi dell'Unione interessati hanno i seguenti obiettivi:

   a) verificare se i requisiti per la protezione delle ICUE previsti dal presente regolamento sono soddisfatti e, di conseguenza, se le misure attuate sono efficaci;

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

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

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

3. Al termine della visita di valutazione, il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate svolge i seguenti compiti:

   a) redigere una relazione contenente le principali conclusioni della valutazione;

   b) chiedere il parere del comitato per la sicurezza delle informazioni di cui all'articolo 6, paragrafo 8, in merito alla relazione;

   c) inviare la relazione all'autorità di sicurezza dell'istituzione o dell'organo dell'Unione visitato affinché vi sia dato seguito.

4. Qualora la relazione proponga azioni correttive o formuli raccomandazioni, è organizzata una visita di follow-up per verificare se tali azioni siano state adottate o se le raccomandazioni siano state seguite.

Articolo 54

Condivisione di ICUE

1. Un'istituzione o un organo dell'Unione può condividere ICUE con un'altra istituzione o un altro organo dell'Unione se sono soddisfatte le seguenti condizioni:

   a) sussiste una comprovata necessità di scambio;

   b) è stata effettuata una visita di valutazione presso l'istituzione o l'organo dell'Unione in questione, conformemente all'articolo 53, il cui esito certifica la capacità di tale istituzione o organo dell'Unione di trattare e conservare un livello specifico di ICUE;

   c) l'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione decide che può condividere informazioni classificate fino a un livello specifico con altre istituzioni e organi dell'Unione certificati.

2. Il segretariato del gruppo di coordinamento redige un elenco dei livelli di ICUE che possono essere trattati e conservati da ogni istituzione e organo dell'Unione che soddisfa le condizioni di cui al paragrafo 1, lettere b) e c). Esso aggiorna periodicamente tale elenco.

Articolo 55

Accordi sulla sicurezza delle informazioni

1. Qualora sia necessario scambiare informazioni classificate con un paese terzo o un'organizzazione internazionale a lungo termine, l'istituzione o l'organo competente si adopera per negoziare e concludere un accordo sulla sicurezza delle informazioni, conformemente all'articolo 218 del trattato sul funzionamento dell'Unione europea.

2. Gli accordi sulla sicurezza delle informazioni stabiliscono i principi di base e le norme minime che disciplinano lo scambio di informazioni classificate tra l'Unione e un paese terzo o un'organizzazione internazionale.

3. Gli accordi sulla sicurezza delle informazioni prevedono modalità tecniche di attuazione da concordare tra le competenti autorità di sicurezza delle istituzioni e degli organi dell'Unione pertinenti e la competente autorità di sicurezza del paese terzo o dell'organizzazione internazionale interessati.

4. Prima dell'approvazione delle modalità tecniche di attuazione di cui al paragrafo 3, il sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate effettua una visita di valutazione conformemente all'articolo 57.

Articolo 56

Intese amministrative con paesi terzi e organizzazioni internazionali

1. Qualora il rispettivo regolamento interno o atto istitutivo ne preveda la possibilità, le istituzioni e gli organi dell'Unione possono concludere un'intesa amministrativa con i loro omologhi di un paese terzo o un'organizzazione internazionale, previa informazione del sottogruppo sulla condivisione di ICUE e lo scambio di informazioni classificate e purché siano soddisfatte le seguenti condizioni:

   a) l'istituzione o l'organo dell'Unione in questione necessita di scambiare a lungo termine informazioni classificate in generale di livello non superiore a RESTREINT UE/EU RESTRICTED con l'omologo di un paese terzo o un'organizzazione internazionale;

   b) l'istituzione o l'organo dell'Unione in questione soddisfa le condizioni di cui all'articolo 54, paragrafo 1;

   c) la relazione sulla visita di valutazione di cui all'articolo 57 certifica che l'omologo pertinente del paese terzo o dell'organizzazione internazionale in questione ha la capacità di trattare e conservare un livello specifico di ICUE.

2. Prima di concludere un'intesa amministrativa, è effettuata una visita di valutazione conformemente ai principi di cui all'articolo 57. L'istituzione o l'organo dell'Unione che persegue l'intesa amministrativa può chiedere al sottogruppo sulla condivisione di ICUE di effettuare la visita di valutazione per suo conto o di partecipare alla visita.

3. L'autorità di sicurezza dell'istituzione o dell'organo dell'Unione che persegue l'intesa amministrativa decide in merito alle condizioni specifiche che disciplinano lo scambio nonché al livello massimo di ICUE che può essere scambiato. Tale livello non è superiore a quello stabilito per la condivisione di ICUE con altre istituzioni e altri organi dell'Unione, conformemente all'articolo 54, e, se del caso, non dovrebbe essere superiore a quello previsto da un accordo sulla sicurezza delle informazioni con lo stesso paese terzo o la stessa organizzazione internazionale.

Articolo 57

Visite di valutazione per lo scambio di informazioni classificate con paesi terzi e organizzazioni internazionali

1. È effettuata una visita di valutazione presso un paese terzo o un'organizzazione internazionale per stabilire se un'istituzione o un organo dell'Unione possa scambiare informazioni classificate con il paese terzo o l'organizzazione internazionale in questione.

2. Scopo della visita di valutazione è valutare l'efficacia delle norme e procedure di sicurezza del paese terzo o dell'organizzazione internazionale interessati per quanto riguarda la protezione delle ICUE a un livello specifico. La visita di valutazione è effettuata di comune accordo con il paese terzo o l'organizzazione internazionale in questione.

3. Le visite di valutazione valutano almeno quanto segue:

   a) il quadro normativo applicabile per proteggere le informazioni classificate e la sua adeguatezza per proteggere le ICUE a un livello specifico;

   b) eventuali aspetti specifici della politica di sicurezza e del modo in cui è organizzata la sicurezza nel paese 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;

   d) le procedure di nulla osta di sicurezza relative al livello ICUE da comunicare.

4. Prima che le ICUE siano effettivamente comunicate al paese terzo o all'organizzazione internazionale in questione, il comitato per la sicurezza delle informazioni di cui all'articolo 6, paragrafo 8, riceve una relazione sui risultati di tali visite. Se del caso, la relazione è condivisa anche con l'istituzione o l'organo dell'Unione in questione.

5. Le autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione comunicano al paese terzo o all'organizzazione internazionale la data a partire dalla quale sono in grado di scambiare ICUE nonché il livello massimo di ICUE che possono essere scambiate in forma cartacea o con mezzi elettronici.

6. Ove sussistano le seguenti condizioni sono organizzate visite di follow-up:

   a) è necessario innalzare il livello di ICUE che può essere scambiato;

   b) l'istituzione o l'organo dell'Unione in questione è stato informato di modifiche fondamentali delle disposizioni di sicurezza del paese terzo o dell'organizzazione internazionale che potrebbero avere ripercussioni sulle modalità di protezione delle ICUE;

c) si è verificato un grave incidente di sicurezza delle informazioni che ha comportato la divulgazione non autorizzata di ICUE.

Articolo 58

Comunicazione eccezionale ad hoc di ICUE

1. In assenza di un accordo sulla sicurezza delle informazioni o di un'intesa amministrativa, se un'istituzione o un organo dell'Unione ravvisa una necessità eccezionale di comunicare ICUE a un'altra istituzione o un altro organo dell'Unione o a un paese terzo o a un'organizzazione internazionale, oppure

   se è stato concluso un accordo sulla sicurezza delle informazioni o un'intesa amministrativa e un'istituzione o un organo dell'Unione ravvisa la necessità eccezionale di comunicare ICUE di livello superiore a quello già previsto dall'accordo o dall'intesa, l'istituzione o l'organo dell'Unione che fornisce le ICUE segue la seguente procedura:

   a) per quanto possibile, verifica con le autorità di sicurezza del paese terzo, dell'organizzazione internazionale o dell'istituzione o dell'organo dell'Unione ricevente che le loro normative, strutture e procedure di sicurezza possano garantire che le ICUE comunicate siano protette secondo norme non meno rigorose di quelle previste dal presente regolamento;

   b) chiede il parere del comitato per la sicurezza delle informazioni di cui all'articolo 6, paragrafo 8, sulla base della verifica effettuata a norma della lettera a), a meno che le circostanze operative richiedano una comunicazione ad hoc immediata, nel qual caso il comitato per la sicurezza delle informazioni è informato successivamente.

2. Tutti i documenti comunicati a norma del presente articolo recano un contrassegno di divulgabilità indicante il paese terzo, l'organizzazione internazionale o l'istituzione o l'organo dell'Unione cui sono stati comunicati.

3. Prima o al momento dell'effettiva comunicazione, l'istituzione o l'organo dell'Unione che fornisce le ICUE chiede alla parte ricevente di impegnarsi per iscritto a proteggere le ICUE che riceve. Se del caso, le è richiesto di impegnarsi a proteggere le ICUE conformemente ai principi di base e alle norme minime di cui al presente regolamento.

Capo 6
Disposizioni finali

Articolo 59

Attuazione

1. Il gruppo di coordinamento elabora orientamenti in materia di sicurezza delle informazioni per l'attuazione del presente regolamento.

2. In base alle proprie esigenze specifiche, le istituzioni e gli organi dell'Unione possono adottare norme interne per l'attuazione del presente regolamento, conformemente all'articolo 8, paragrafo 2.

Articolo 60

Disposizioni transitorie

1. Le norme interne sulla sicurezza delle informazioni adottate dalle singole istituzioni o dai singoli organi dell'Unione prima del [gg/mm/aaaa data di applicazione] sono riesaminate entro [tre anni dall'entrata in vigore del presente regolamento].

2. Tutte le istituzioni e tutti gli organi dell'Unione che sono stati valutati idonei a trattare e conservare ICUE dalla Commissione o dal Consiglio o dal SEAE prima del [gg/mm/aaaa data di applicabilità] sono considerati conformi alle condizioni di cui all'articolo 19, paragrafo 1.

3. Tutti le intese amministrative concluse dalle istituzioni e dagli organi dell'Unione con paesi terzi e organizzazioni internazionali prima del [gg/mm/aaaa data di applicazione] restano valide.

4. Qualora gli Stati membri sul cui territorio i beneficiari della convenzione di sovvenzione della Commissione nell'ambito del programma europeo di sviluppo del settore industriale della difesa abbiano deciso di dotarsi di un quadro di sicurezza specifico per la protezione e il trattamento delle informazioni classificate a livello nazionale in relazione alla convenzione di sovvenzione in questione, la Commissione, nell'applicare le procedure di sicurezza industriale di cui al presente regolamento, rispetterà tale quadro di sicurezza fino al termine del ciclo di vita della convenzione di sovvenzione.

Articolo 61

Monitoraggio e valutazione

1. Entro il [gg/mm/aaaa tre anni dalla data di applicazione], la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'attuazione del presente regolamento.

2. Trascorsi almeno [cinque anni dalla data di applicazione] e successivamente ogni cinque anni, la Commissione effettua una valutazione del presente regolamento e presenta al Parlamento europeo e al Consiglio una relazione sulle principali conclusioni.

Articolo 62

Entrata in vigore e applicazione

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

2. Esso si applica a decorrere dal [data: il primo giorno del mese successivo al periodo di due anni dalla data di entrata in vigore].

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

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
[...]	*[...]*

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. La proposta/iniziativa riguarda:

1.4. Obiettivi

1.4.1. Obiettivi generali

1.4.2. Obiettivi specifici

1.4.3. Risultati e incidenza previsti

1.4.4. Indicatori di prestazione

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

1.5.3. Insegnamenti tratti da esperienze analoghe

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

1.6. Durata e incidenza finanziaria della proposta/iniziativa

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione

1.2. Settore/settori interessati

Amministrazione pubblica europea

Le norme di sicurezza delle informazioni delle istituzioni e degli organi dell'Unione dovrebbero costituire, nel loro insieme, un quadro generale completo e coerente all'interno dell'amministrazione europea per la protezione delle informazioni e garantire l'equivalenza dei principi di base e delle norme minime. Anche il livello di protezione riconosciuto alle informazioni dovrebbe essere equivalente in tutte le istituzioni e tutti gli organi dell'Unione.

1.3. La proposta/iniziativa riguarda:

☑una nuova azione

☐ una nuova azione a seguito di un progetto pilota/un'azione preparatoria[32]

☐ la proroga di un'azione esistente

☐ la fusione o il riorientamento di una o più azioni verso un'altra/una nuova azione

1.4. Obiettivi

1.4.1. Obiettivi generali

L'obiettivo generale dell'iniziativa è stabilire norme di sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione allo scopo di assicurare una protezione rafforzata e continua dalle minacce in evoluzione che incombono sulle loro informazioni.

1.4.2. Obiettivi specifici

• OBIETTIVO SPECIFICO 1: stabilire categorie armonizzate e complete di informazioni, nonché requisiti comuni in materia di trattamento per tutte le informazioni trattate dall'amministrazione europea, e facilitare lo scambio sicuro di informazioni tra le istituzioni e gli organi dell'Unione, riducendo al minimo l'impatto sugli Stati membri.

• OBIETTIVO SPECIFICO 2: garantire che tutte le istituzioni e tutti gli organi dell'Unione individuino eventuali lacune in materia di sicurezza nelle loro procedure e attuino le misure richieste per garantire parità di condizioni in materia di sicurezza delle informazioni.

• OBIETTIVO SPECIFICO 3: istituire un sistema snello di cooperazione in materia di sicurezza delle informazioni tra le istituzioni e gli organi dell'Unione, in grado di

[32] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

promuovere una cultura coerente della sicurezza delle informazioni in tutta l'amministrazione europea.

• OBIETTIVO SPECIFICO 4: modernizzare le politiche in materia di sicurezza delle informazioni a tutti i livelli di classifica/categorizzazione, per tutte le istituzioni e tutti gli organi dell'Unione, tenendo conto della trasformazione digitale e dello sviluppo del telelavoro come pratica strutturale.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

La proposta avrà i seguenti effetti sulle istituzioni e sugli organi dell'Unione:

– revisione delle loro norme e procedure interne al fine di adattarle al regolamento;

– categorizzazione di tutte le informazioni trattate conformemente al regime previsto dal regolamento;

– garantire che i loro sistemi di comunicazione e informazione siano conformi ai requisiti stabiliti dal regolamento;

– partecipare al gruppo di coordinamento interistituzionale per la sicurezza delle informazioni ("gruppo di coordinamento").

Gli Stati membri trarranno benefici dal presente regolamento in quanto la cooperazione con le istituzioni e gli organi dell'Unione in tutti i settori pertinenti (sicurezza del personale, sicurezza industriale o condivisione delle informazioni) si baserebbe sugli stessi concetti, norme e procedure.

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati

Indicatori pertinenti per l'obiettivo specifico 1

– Adozione di linee guida adeguate

– Attuazione di nuovi contrassegni

– Pubblicazione di istruzioni di trattamento aggiornate per tutte le categorie di informazioni

– Attuazione di sistemi comuni che trattano informazioni sensibili non classificate e ICUE

Indicatori pertinenti per l'obiettivo specifico 2

– Numero di raccomandazioni formulate/attuate

– Numero di fughe di informazioni tra le istituzioni e gli organi

Indicatori pertinenti per l'obiettivo specifico 3

– Statistiche sugli appalti centralizzati rispetto a quelli locali

– Rapporti di ispezione

– Numero di domande trattate dal segretariato del gruppo di coordinamento per la sicurezza delle informazioni

Indicatori pertinenti per l'obiettivo specifico 4

- Numero di utenti che seguono una formazione
- Livello di sensibilizzazione del personale alle norme di sicurezza delle informazioni
- Percentuale del personale che può lavorare con attrezzature di telelavoro sicure

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

L'attuazione di questa iniziativa seguirà un approccio graduale come segue:

- 2022/2023: adozione del regolamento ed entrata in vigore
- 2024/2025: riesame, da parte di tutte le istituzioni e tutti gli organi dell'Unione, delle loro norme interne di sicurezza delle informazioni al fine di adeguarle al regolamento
- 2025: lavori organizzativi per la costituzione del gruppo di coordinamento e del suo segretariato, nonché dei sottogruppi tecnici
- 2024/2025: inizio dell'applicazione del regolamento
- 2025/2026: adozione del regolamento interno del gruppo di coordinamento e dei sottogruppi tecnici
- 2026-2028: lavori sui documenti di orientamento a sostegno dell'attuazione del regolamento e scambio delle migliori pratiche tra istituzioni e organi
- 2029/2030: preparazione della prima valutazione del regolamento (ogni cinque anni dalla data di applicazione)
- 2030: prima valutazione del regolamento

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

L'iniziativa contribuisce a garantire che le istituzioni e gli organi dell'Unione siano assistiti nei loro compiti da un'amministrazione aperta, efficace ed indipendente. Essa si aggiunge agli sforzi nazionali generali degli Stati membri nel settore della sicurezza dell'UE proteggendo le istituzioni e gli organi dalle interferenze esterne e dalle attività di spionaggio.

1.5.3. Insegnamenti tratti da esperienze analoghe

N/A

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

Il progetto richiede la riassegnazione/assegnazione di 2 ETP per il segretariato del gruppo di coordinamento per la sicurezza delle informazioni.

Altri progetti, come lo sviluppo di strumenti comuni e la centralizzazione di alcune attività, sono già parzialmente in corso e sono coperti dagli SLA e dai contratti quadro.

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

Cfr. la sezione precedente.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **durata limitata**

– ☐ in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ incidenza finanziaria dal AAAA al AAAA per gli stanziamenti di impegno e dal AAAA al AAAA per gli stanziamenti di pagamento

– ☑ **durata illimitata**

1.7. Modalità di gestione previste[33]

☑ **Gestione diretta** a opera della Commissione e di ogni istituzione e organo dell'Unione

– ☑ a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☐ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V TUE e indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

[33] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

Ogni cinque anni il regolamento sarà valutato e la Commissione riferirà in merito al Consiglio e al Parlamento europeo.

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

Il regolamento stabilisce le norme di sicurezza delle informazioni per tutte le istituzioni e tutti gli organi dell'Unione. Il monitoraggio della sua corretta attuazione avverrà attraverso un gruppo di coordinamento che coinvolgerà tutte le autorità di sicurezza delle istituzioni e degli organi.

L'autorità di sicurezza di ogni istituzione od organo resta pienamente responsabile della sicurezza, nel rispetto del quadro di controllo interno esistente di ogni istituzione o organo.

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

Il regolamento creerà una base di riferimento per le norme in materia di sicurezza delle informazioni e garantirà la trasparenza delle misure di sicurezza per gli scambi di informazioni tra le istituzioni e gli organi dell'Unione, riducendo in tal modo i rischi relativi alla sicurezza delle informazioni in tutti i settori.

Il regolamento è conforme alle norme di controllo interno e prevede un approccio basato sul rischio per l'elaborazione delle politiche.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

Saranno applicabili i meccanismi di controllo esistenti per le istituzioni e gli organi. La conformità al regolamento e i rischi relativi alla sicurezza delle informazioni dovrebbero essere segnalati nelle relazioni annuali sui rischi delle istituzioni e degli organi.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

N/A

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Tipo di spesa	Partecipazione			
	Numero	Diss./Non diss.[34]	di paesi EFTA[35]	di paesi candidati[36]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
H7	20 01 02 01	Non diss.	NO	NO	NO	NO

- Nuove linee di bilancio di cui è chiesta la creazione

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Tipo di spesa	Partecipazione			
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	Nessuna		SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

34 Diss. = stanziamenti dissociati/Non diss. = stanziamenti non dissociati.
35 EFTA: Associazione europea di libero scambio.
36 Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

– ☑ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Numero	

DG: <…….>			Anno **N**[37]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
• Stanziamenti operativi										
Linea di bilancio[38]	Impegni	(1a)								
	Pagamenti	(2 a)								
Linea di bilancio	Impegni	(1b)								
	Pagamenti	(2b)								
Stanziamenti amministrativi finanziati dalla dotazione di programmi specifici[39]										
Linea di bilancio		(3)								
TOTALE stanziamenti per la DG <….>	Impegni	=1a+1b +3								
	Pagamenti	=2a+2b +3								

37 L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

38 Secondo la nomenclatura di bilancio ufficiale.

39 Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

• TOTALE stanziamenti operativi	Impegni	(4)								
	Pagamenti	(5)								
• TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici		(6)								
TOTALE degli stanziamenti per la RUBRICA <….> del quadro finanziario pluriennale	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Se la proposta/iniziativa incide su più rubriche operative, ricopiare nella sezione sotto:

• TOTALE stanziamenti operativi (tutte le rubriche operative)	Impegni	(4)								
	Pagamenti	(5)								
TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici (tutte le rubriche operative)		(6)								
TOTALE stanziamenti a titolo delle rubriche da 1 a 6 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Rubrica del quadro finanziario pluriennale	**7**	"Spese amministrative"

Sezione da compilare utilizzando i "dati di bilancio di natura amministrativa" che saranno introdotti nell'allegato della scheda finanziaria legislativa (allegato V delle norme interne), caricato su DECIDE a fini di consultazione interservizi.

Mio EUR (al terzo decimale)

		Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
DG: HR							
• Risorse umane		0,314	0,314	0,314	0,314	0,314	**1,570**
• Altre spese amministrative							
TOTALE DG<….>	Stanziamenti	0,314	0,314	0,314	0,314	0,314	**1,570**

TOTALE stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	0,314	0,314	0,314	0,314	0,314	**1,570**

Mio EUR (al terzo decimale)

		Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
TOTALE stanziamenti a titolo delle rubriche da 1 a 7 del quadro finanziario pluriennale	Impegni	0,314	0,314	0,314	0,314	0,314	**1,570**
	Pagamenti	0,314	0,314	0,314	0,314	0,314	**1,570**

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **N**		Anno **N+1**		Anno **N+2**		Anno **N+3**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**	
	RISULTATI																	
	Tipo[40]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[41]…																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		
- Risultato																		
Totale parziale dell'obiettivo specifico 2																		
TOTALE																		

40 I risultati sono i prodotti e i servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

41 Come descritto nella sezione 1.4.2. "Obiettivi specifici..."

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
RUBRICA 7 del quadro finanziario pluriennale						
Risorse umane	0,314	0,314	0,314	0,314	0,314	**1,570**
Altre spese amministrative						
Totale parziale RUBRICA 7 del quadro finanziario pluriennale	0,314	0,314	0,314	0,314	0,314	**1,570**

Esclusa la RUBRICA 7[42] del quadro finanziario pluriennale						
Risorse umane						
Altre spese amministrative						
Totale parziale al di fuori della RUBRICA 7 del quadro finanziario pluriennale						

TOTALE	0,314	0,314	0,314	0,314	0,314	**1,570**

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese amministrative è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[42] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☑ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

		Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**
20 01 02 01 (sede e uffici di rappresentanza della Commissione)		2	2	2	2	2
20 01 02 03 (delegazioni)						
01 01 01 01 (ricerca indiretta)						
01 01 01 11 (ricerca diretta)						
Altre linee di bilancio (specificare)						
20 02 01 (AC, END, INT della dotazione globale)						
20 02 03 (AC, AL, END, INT e JPD nelle delegazioni)						
XX 01 xx **yy zz**[43]	- in sede					
	- nelle delegazioni					
01 01 01 02 (AC, END, INT - ricerca indiretta)						
01 01 01 12 (AC, END, INT - ricerca diretta)						
Altre linee di bilancio (specificare)						
TOTALE		**2**	**2**	**2**	**2**	**2**

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Segretariato del gruppo di coordinamento per la sicurezza delle informazioni: 1 funzionario AD + 1 funzionario AST
Personale esterno	

[43] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

La proposta/iniziativa:

– ☑ può essere interamente finanziata mediante riassegnazione all'interno della pertinente rubrica del quadro finanziario pluriennale (QFP).

La proposta prevede l'assegnazione di due membri del personale al segretariato permanente del gruppo di coordinamento interistituzionale, in seno all'unità HR.DS.

– ☐ comporta l'uso del margine non assegnato della pertinente rubrica del QFP e/o l'uso degli strumenti speciali definiti nel regolamento QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate, gli importi corrispondenti e gli strumenti proposti.

– ☐ comporta una revisione del QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– ☑ non prevede cofinanziamenti da terzi

– ☐ prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**[44]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Totale
Specificare l'organismo di cofinanziamento					
TOTALE stanziamenti cofinanziati					

Osservazione: la proposta intensificherà le attuali cooperazioni in materia di sicurezza delle informazioni attraverso gli SLA.

[44] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

3.3. Incidenza prevista sulle entrate

– ☑ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

☐ sulle risorse proprie

☐ su altre entrate

indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[45]			
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**

Per quanto riguarda le entrate con destinazione specifica, precisare la o le linee di spesa interessate.

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni)

[45] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.