DECISIONI

DECISIONE (UE, Euratom) 2017/46 DELLA COMMISSIONE

del 10 gennaio 2017

sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea

LA COMMISSIONE EUROPEA,

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

visto il trattato che istituisce la Comunità europea dell'energia atomica,

considerando quanto segue:

(1) I sistemi di comunicazione e informazione della Commissione sono parte integrante del funzionamento della Commissione e gli incidenti legati alla sicurezza informatica possono avere un grave impatto sull'attività della Commissione e di terzi, tra cui i cittadini, le imprese e gli Stati membri.

(2) Sono numerose le minacce che possono danneggiare la riservatezza, l'integrità o la disponibilità dei sistemi di comunicazione e informazione della Commissione e dei dati da essi trattati. Tali minacce includono incidenti, errori, attacchi dolosi ed eventi naturali, e devono essere riconosciute come rischi operativi.

(3) I sistemi di comunicazione e informazione devono essere dotati di un livello di protezione commisurato alla probabilità, all'impatto e alla natura dei rischi ai quali sono esposti.

(4) La sicurezza informatica della Commissione dovrebbe assicurare che i sistemi di comunicazione e informazione della Commissione proteggano le informazioni che trattano e che funzionino correttamente e tempestivamente sotto il controllo degli utenti legittimi.

(5) La politica in materia di sicurezza informatica della Commissione dovrebbe essere attuata in modo coerente con le politiche in materia di sicurezza della Commissione.

(6) La direzione «Sicurezza» della direzione generale Risorse umane e sicurezza ha la responsabilità generale della sicurezza alla Commissione sotto l'autorità e la responsabilità del membro della Commissione responsabile della sicurezza.

(7) L'approccio della Commissione dovrebbe prendere in considerazione le iniziative politiche e normative in materia di sicurezza delle reti e dell'informazione nonché le norme e le buone pratiche del settore per conformarsi a tutte le normative pertinenti e consentire l'interoperabilità e la compatibilità.

(8) I servizi della Commissione responsabili dei sistemi di comunicazione e informazione dovrebbero elaborare e attuare misure adeguate. Le misure di sicurezza informatica per proteggere i sistemi in questione dovrebbero essere coordinate a livello della Commissione per assicurarne l'efficienza e l'efficacia.

(9) Le norme e procedure per l'accesso alle informazioni in tema di sicurezza informatica, compresa la gestione degli incidenti di sicurezza informatica, dovrebbero essere proporzionate alla minaccia per la Commissione o il suo personale e conformi ai principi di cui al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([1]), concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, e tenuto conto del principio del segreto professionale di cui all'articolo 339 del TFUE.

([1]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

(10) Le politiche e le norme per i sistemi di comunicazione e informazione che trattano informazioni classificate dell'UE (ICUE), informazioni sensibili non classificate e informazioni non classificate devono essere pienamente conformi alle decisioni (UE, Euratom) 2015/443 ([1]) e 2015/444 ([2]) della Commissione.

(11) La Commissione deve riesaminare e aggiornare le disposizioni relative alla sicurezza dei sistemi di comunicazione e informazione da essa utilizzati.

(12) È quindi necessario abrogare la decisione C(2006) 3602 della Commissione,

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e campo di applicazione

1. La presente decisione si applica a tutti i sistemi di comunicazione e informazione (CIS) che sono posseduti, acquistati, gestiti oppure operati da o per conto della Commissione e a ogni utilizzo di tali CIS da parte della Commissione.

2. La presente decisione stabilisce gli obiettivi, i principi, l'organizzazione e le responsabilità fondamentali in relazione alla sicurezza dei CIS e, in particolare, per i servizi della Commissione che li possiedono, acquistano, gestiscono oppure operano, compresi i CIS forniti da un prestatore di servizi informatici interni. Quando un CIS è fornito, posseduto, gestito oppure operato da una terza parte esterna sulla base di un accordo bilaterale o di un contratto con la Commissione, i termini dell'accordo o del contratto sono conformi alla presente decisione.

3. La presente decisione si applica a tutti i servizi della Commissione e delle agenzie esecutive. Quando un CIS è utilizzato da altri organi e istituzioni sulla base di un accordo bilaterale con la Commissione, i termini dell'accordo sono conformi alla presente decisione.

4. Fatte salve le indicazioni specifiche relative a particolari categorie del personale, la presente decisione si applica ai membri della Commissione, al personale della Commissione che rientra nel campo di applicazione dello statuto dei funzionari dell'Unione europea («lo statuto») e del regime applicabile agli altri agenti dell'Unione (il «RAA») ([3]), agli esperti nazionali distaccati presso la Commissione (gli «END») ([4]), ai prestatori di servizi esterni e al loro personale, ai tirocinanti e ai singoli che hanno accesso ai CIS nel campo di applicazione della presente decisione.

5. La presente decisione si applica all'Ufficio europeo per la lotta antifrode (OLAF), nella misura in cui essa è compatibile con la legislazione dell'Unione e con la decisione della Commissione 1999/352/CE, CECA, Euratom ([5]). In particolare, le misure di cui alla presente decisione, comprese le istruzioni, le ispezioni, le indagini e le misure equivalenti, possono non applicarsi al CIS dell'Ufficio nei casi in cui ciò non è compatibile con l'indipendenza della funzione d'indagine dell'Ufficio e/o la riservatezza delle informazioni raccolte dall'Ufficio nell'esercizio di tale funzione.

Articolo 2

Definizioni

Ai fini della presente decisione si intende per:

(1) «responsabile», il fatto di assumersi la responsabilità per azioni, decisioni e risultati;

([1]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).
([2]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).
([3]) Regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio, del 29 febbraio 1968, che definisce lo statuto dei funzionari delle Comunità europee nonché il regime applicabile agli altri agenti di tali Comunità, ed istituisce speciali misure applicabili temporaneamente ai funzionari della Commissione (GU L 56 del 4.3.1968, pag. 1).
([4]) Decisione della Commissione del 12 novembre 2008, che stabilisce le regole per il distacco di esperti nazionali e di esperti nazionali in formazione professionale [C(2008) 6866 final].
([5]) Decisione 1999/352/CE, CECA, Euratom della Commissione, del 28 aprile 1999, che istituisce l'Ufficio europeo per la lotta antifrode (OLAF) (GU L 136 del 31.5.1999, pag. 20).

(2) «CERT-UE», la squadra di pronto intervento informatico delle istituzioni e agenzie dell'UE. La sua missione consiste nell'aiutare le istituzioni europee a proteggersi dagli attacchi intenzionali e dolosi che potrebbero danneggiare l'integrità del patrimonio informatico e ledere gli interessi dell'UE. Il campo di applicazione delle attività di CERT-UE comprende la prevenzione, l'individuazione del problema, la risposta e il ripristino;

(3) «servizio della Commissione», le direzioni generali, i servizi della Commissione o i gabinetti dei membri della Commissione;

(4) «autorità di sicurezza della Commissione», il ruolo di cui alla decisione 2015/444;

(5) «sistema di comunicazione e informazione» o «CIS», ogni sistema che consente il trattamento delle informazioni in forma elettronica, compreso l'insieme delle risorse necessarie al suo funzionamento, nonché l'infrastruttura, l'organizzazione, il personale e le risorse d'informazione. La presente definizione comprende le applicazioni commerciali, i sistemi informatici comuni, i servizi esternalizzati e i dispositivi degli utenti finali;

(6) «organo di gestione interno» (CMB), l'organo che fornisce il massimo livello di sorveglianza della gestione interna per le questioni amministrative e operative della Commissione;

(7) «proprietario dei dati», la persona responsabile di assicurare la protezione e l'utilizzo di un set di dati specifico trattato da un CIS;

(8) «set di dati», una serie di informazioni per uno specifico processo o attività della Commissione;

(9) «procedura di emergenza», un insieme predefinito di metodi e responsabilità per rispondere a situazioni di emergenza al fine di prevenire gravi conseguenze per la Commissione;

(10) «politica di sicurezza delle informazioni», una serie di obiettivi in materia di sicurezza delle informazioni, che sono o devono essere stabiliti, attuati e controllati. Comprende, tra l'altro, le decisioni (UE, Euratom) 2015/444 e 2015/443;

(11) «comitato direttivo per la sicurezza delle informazioni» (ISBB), l'organo di gestione che sostiene l'organo di gestione interno nelle sue mansioni connesse alla sicurezza informatica;

(12) «prestatore interno di servizi informatici», un servizio della Commissione che fornisce servizi informatici condivisi;

(13) «sicurezza informatica» o «sicurezza dei CIS», il mantenimento della riservatezza, dell'integrità e della disponibilità dei CIS e delle serie di dati che essi trattano;

(14) «orientamenti in materia di sicurezza informatica», misure raccomandate ma facoltative volte a sostenere gli standard di sicurezza informatica o a servire da riferimento quando non vi sono norme applicabili;

(15) «incidente di sicurezza informatica», un evento che potrebbe compromettere la riservatezza, l'integrità o la disponibilità di un CIS;

(16) «misura di sicurezza informatica», una misura tecnica oppure organizzativa volta a ridurre i rischi per la sicurezza informatica;

(17) «esigenza di sicurezza informatica», una definizione precisa e univoca dei livelli di riservatezza, integrità e disponibilità associati a un sistema d'informazione o a un sistema informatico al fine di determinare il livello di protezione richiesto;

(18) «obiettivo di sicurezza informatica», una dichiarazione d'intenti per contrastare minacce specifiche e/o soddisfare determinati requisiti o ipotesi di sicurezza organizzativa;

(19) «piano di sicurezza informatica», la documentazione delle misure di sicurezza informatica necessarie per soddisfare le esigenze di sicurezza di un CIS;

(20) «politica di sicurezza informatica», una serie di obiettivi in materia di sicurezza informatica, che sono o devono essere stabiliti, attuati e controllati. Comprende la presente decisione e le relative norme di attuazione;

(21) «requisito di sicurezza informatica», un'esigenza di sicurezza informatica formalizzata mediante un processo predefinito:

(22) «rischio in materia di sicurezza informatica», un effetto che una minaccia per la sicurezza informatica potrebbe causare a un CIS sfruttandone la vulnerabilità. In quanto tale, un rischio in materia di sicurezza informatica è caratterizzato da due fattori: 1) l'incertezza, ad esempio la probabilità che una minaccia per la sicurezza informatica provochi un evento indesiderato, e 2) l'impatto, ossia le conseguenze che un simile evento indesiderato potrebbe avere su un CIS;

(23) «norme di sicurezza informatica», specifiche misure obbligatorie in materia di sicurezza informatica che contribuiscono a far rispettare e sostenere la politica in materia di sicurezza informatica;

(24) «strategia di sicurezza informatica», una serie di progetti e attività volti a conseguire gli obiettivi della Commissione e che sono stati stabiliti, attuati e controllati;

(25) «minaccia per la sicurezza informatica», un fattore che potrebbe portare a un evento indesiderato che potrebbe danneggiare un CIS. Tali minacce possono essere accidentali o intenzionali e sono caratterizzate da elementi di minaccia, obiettivi potenziali e metodologie d'attacco;

(26) «responsabile della sicurezza informatica a livello locale» (LISO), il funzionario responsabile del collegamento per la sicurezza informatica di un servizio della Commissione;

(27) «dati personali», «trattamento dei dati personali», «responsabile del trattamento» e «archivio dei dati personali» hanno lo stesso significato di cui al regolamento (CE) n. 45/2001, in particolare l'articolo 2;

(28) «trattamento delle informazioni», tutte le funzioni di un CIS con riferimento ai set di dati, compresi la creazione, la modifica, la visualizzazione, lo stoccaggio, il trasporto, la cancellazione e l'archiviazione delle informazioni. Il trattamento delle informazioni può essere fornito da un CIS come una serie di funzionalità per gli utenti e come servizi informatici ad altri CIS;

(29) «segreto professionale», la protezione dei dati commerciali del tipo coperto dal segreto professionale, in particolare informazioni relative a imprese, alle loro relazioni commerciali o alle loro componenti di costo di cui all'articolo 339 del TFUE;

(30) «responsabile», l'obbligo di agire e prendere decisioni per conseguire i risultati richiesti;

(31) «sicurezza nella Commissione», la sicurezza delle persone, delle risorse e delle informazioni alla Commissione, in particolare l'incolumità delle persone e l'integrità delle risorse, l'integrità, la riservatezza e la disponibilità delle informazioni e dei sistemi di comunicazione e informazione, nonché il funzionamento senza ostacoli delle attività operative della Commissione;

(32) «servizio informatico condiviso», il servizio che un CIS fornisce ad altri CIS nel trattamento delle informazioni;

(33) «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 CIS;

(34) «utente», qualsiasi persona fisica utilizzi funzionalità fornite da un CIS, sia all'interno che all'esterno della Commissione.

Articolo 3

Principi per la sicurezza informatica alla Commissione

1. La sicurezza informatica alla Commissione si basa sui principi di legalità, trasparenza, proporzionalità e responsabilità.

2. Le questioni di sicurezza informatica sono prese in considerazione fin dall'inizio dell'elaborazione e attuazione dei CIS della Commissione. A tal fine, la direzione generale dell'Informatica e la direzione generale Risorse umane e sicurezza sono coinvolte per i rispettivi ambiti di competenza.

3. Una sicurezza informatica efficace assicura livelli adeguati di:

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

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

c) riservatezza: la proprietà per cui l'informazione non è divulgata a persone, entità o procedure non autorizzate;

d) integrità: la proprietà di tutela della precisione e della completezza delle informazioni e delle risorse;

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

f) protezione dei dati personali: la fornitura di garanzie adeguate in relazione ai dati personali nel pieno rispetto del regolamento (CE) n. 45/2001;

g) segreto professionale: la protezione di informazioni del tipo coperte dal segreto professionale, in particolare informazioni relative a imprese, alle loro relazioni commerciali o alle loro componenti di costo di cui all'articolo 339 del TFUE.

4. La sicurezza informatica si basa su un processo di gestione del rischio che intende stabilire i livelli di rischio per la sicurezza e definire le misure di sicurezza per contenerli entro un livello adeguato e con un costo proporzionato.

5. Tutti i CIS sono identificati, assegnati a un proprietario di sistema e registrati in un inventario.

6. I requisiti di sicurezza di tutti i CIS sono determinati sulla base delle loro esigenze di sicurezza e delle esigenze in materia di sicurezza delle informazioni da essi trattate. I CIS che forniscono servizi ad altri CIS possono essere progettati per sostenere determinati livelli di esigenze in materia di sicurezza.

7. I piani di sicurezza informatica e le relative misure di sicurezza sono proporzionati alle esigenze di sicurezza dei CIS.

I processi relativi a questi principi e attività sono ulteriormente dettagliati nelle norme di attuazione.

CAPO 2

ORGANIZZAZIONE E RESPONSABILITÀ

Articolo 4

Organo di gestione interno

L'organo di gestione interno ha la responsabilità generale della gestione della sicurezza informatica complessiva all'interno della Commissione.

Articolo 5

Comitato direttivo per la sicurezza dell'informazione (ISSB)

1. L'ISSB è presieduto dal segretario generale aggiunto competente per la governance della sicurezza informatica della Commissione. I suoi membri rappresentano gli interessi commerciali, tecnologici e di sicurezza di tutti i servizi della Commissione e comprendono rappresentanti della direzione generale dell'Informatica, della direzione generale Risorse umane e sicurezza, della direzione generale del Bilancio e, a rotazione ogni due anni, i rappresentanti di altri quattro servizi della Commissione coinvolti in cui la sicurezza informatica costituisce una grave preoccupazione per le loro operazioni. L'adesione è a livello di alta dirigenza.

2. L'ISSB assiste l'organo di gestione interno nelle sue mansioni in materia di sicurezza informatica. Ha la responsabilità operativa della gestione della sicurezza informatica complessiva all'interno della Commissione.

3. L'ISBB formula raccomandazioni in materia di politica di sicurezza informatica da adottare da parte della Commissione.

4. Esamina e riferisce ogni due anni al Consiglio di amministrazione in materia di questioni di governance nonché di temi che riguardano la sicurezza informatica, compresi gli incidenti gravi di sicurezza informatica.

5. Controlla ed esamina l'attuazione globale della presente decisione e riferisce in merito all'organo di gestione interno.

6. Su proposta della direzione generale dell'Informatica, esamina, approva e controlla l'attuazione della strategia di sicurezza in corso. Riferisce in merito all'organo di gestione interno.

7. Monitora, valuta e controlla le modalità di trattamento del rischio per le informazioni interne ed esercita il potere di emanare prescrizioni formali per apportare miglioramenti laddove necessario.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 6

Direzione generale Risorse umane e Sicurezza

Per quanto riguarda la sicurezza informatica, la direzione generale Risorse umane e sicurezza ha le seguenti responsabilità. Essa:

(1) garantisce l'allineamento tra la politica in materia di sicurezza informatica e la politica in materia di sicurezza delle informazioni della Commissione;

(2) istituisce un quadro per l'autorizzazione a utilizzare le tecnologie di crittografia per la conservazione e la trasmissione delle informazioni da parte dei CIS;

(3) informa la direzione generale dell'Informatica in merito a minacce specifiche che potrebbero avere un impatto significativo sulla sicurezza dei CIS e sui set di dati che essi trattano;

(4) svolge ispezioni di sicurezza per verificare la conformità dei CIS della Commissione alla politica di sicurezza e riferirne i risultati all'ISSB;

(5) istituisce un quadro per l'autorizzazione di accesso e le relative norme di sicurezza adeguate per i CIS della Commissione da reti esterne e sviluppa le norme e gli orientamenti di sicurezza informatica in stretta collaborazione con la direzione generale dell'Informatica;

(6) propone principi e norme per l'esternalizzazione dei CIS al fine di mantenere un adeguato controllo sulla sicurezza delle informazioni;

(7) sviluppa le norme di sicurezza informatica e i relativi orientamenti in relazione all'articolo 6, in stretta collaborazione con la direzione generale dell'Informatica.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 7

Direzione generale dell'Informatica

Per quanto riguarda la sicurezza informatica complessiva della Commissione, la direzione generale dell'Informatica ha le seguenti responsabilità. Essa:

(1) sviluppa norme e orientamenti in materia di sicurezza informatica, ad eccezione dei casi di cui all'articolo 6, in stretta collaborazione con la direzione generale Risorse umane e sicurezza, al fine di garantire la coerenza tra la politica in materia di sicurezza informatica e la politica della Commissione in materia di sicurezza delle informazioni, e li propone all'ISSB;

(2) valuta i metodi di gestione dei rischi per la sicurezza informatica, i relativi processi e i risultati di tutti i servizi della Commissione e ne riferisce periodicamente all'ISSB;

(3) sottopone all'esame e all'approvazione dell'ISSB una strategia di sicurezza informatica, che successivamente deve essere adottata dall'organo di gestione interno, e propone un programma, comprendente la pianificazione di progetti e attività per l'attuazione della strategia in materia di sicurezza informatica;

(4) monitora l'esecuzione della strategia della Commissione in materia di sicurezza informatica e riferisce periodicamente in merito all'ISSB;

(5) monitora i rischi in materia di sicurezza informatica e le relative misure attuate dai CIS e riferisce periodicamente in merito all'ISSB;

(6) riferisce periodicamente all'ISSB in merito all'attuazione generale e alla conformità alla presente decisione;

(7) previa consultazione con la direzione generale Risorse umane e sicurezza, richiede ai proprietari del sistema di adottare specifiche misure in materia di sicurezza informatica al fine di attenuare i rischi per la sicurezza informatica dei CIS della Commissione;

(8) assicura la disponibilità di un catalogo adeguato dei servizi in materia di sicurezza informatica della direzione generale dell'Informatica per i proprietari dei sistemi e i proprietari dei dati affinché adempiano alle loro responsabilità in materia di sicurezza informatica e rispettino la politica in materia di sicurezza informatica e le relative norme;

(9) fornisce un'adeguata documentazione ai proprietari dei sistemi e dei dati e si consulta con essi, ove opportuno, sulle misure di sicurezza informatica attuate per i loro servizi informatici al fine di facilitare la conformità alla politica in materia di sicurezza informatica e assistere i proprietari dei sistemi nella gestione dei rischi informatici;

(10) organizza riunioni periodiche della rete dei LISO e li assiste ai fini dello svolgimento dei loro compiti;

(11) definisce le esigenze di formazione e coordina i programmi di formazione sulla sicurezza informatica in collaborazione con i servizi della Commissione, e sviluppa, realizza e coordina le campagne di sensibilizzazione alla sicurezza informatica in stretta collaborazione con la direzione generale Risorse umane;

(12) garantisce che i proprietari dei sistemi, i proprietari dei dati e i diversi ruoli con responsabilità in materia di sicurezza informatica all'interno dei servizi della Commissione siano a conoscenza della politica in materia di sicurezza informatica;

(13) informa la direzione generale Risorse umane e sicurezza in merito a specifici rischi di sicurezza informatica, incidenti ed eccezioni alla politica della Commissione in materia di sicurezza informatica notificati dai proprietari dei sistemi che potrebbero avere un impatto significativo sulla sicurezza alla Commissione;

(14) in merito al proprio ruolo di fornitore di servizi informatici interni, fornisce alla Commissione un catalogo di servizi informatici condivisi capaci di garantire livelli definiti di sicurezza. Ciò sarà effettuato mediante valutazione, gestione e controllo sistematici dei rischi di sicurezza informatica per attuare le misure di sicurezza al fine di raggiungere il livello di sicurezza definito.

I relativi processi e le responsabilità più specifiche sono ulteriormente definiti nelle norme di attuazione.

Articolo 8

Servizi della Commissione

In relazione alla sicurezza informatica nei propri servizi, il capo di ciascun servizio della Commissione:

(1) nomina formalmente per ogni CIS un proprietario del sistema, che è un funzionario o un agente temporaneo, il quale è responsabile della sicurezza informatica di tale CIS e nomina formalmente un proprietario dei dati per ogni set di dati trattati in un CIS che dovrebbe appartenere alla stessa unità amministrativa responsabile del trattamento dei dati per i set di dati soggetti al regolamento (CE) n. 45/2001;

(2) designa formalmente un responsabile della sicurezza informatica a livello locale (LISO), che può svolgere le funzioni in modo indipendente dai proprietari del sistema e dei dati. Un LISO può essere designato per uno o più dei servizi della Commissione;

(3) garantisce la formulazione e l'attuazione di adeguate valutazioni dei rischi per la sicurezza informatica e dei piani per la sicurezza informatica;

(4) garantisce la trasmissione periodica di una sintesi di tali rischi e delle misure in materia di sicurezza informatica alla direzione generale dell'Informatica;

(5) garantisce, con il sostegno della direzione generale dell'Informatica, l'adozione di adeguati processi, procedure e soluzioni per individuare, segnalare e risolvere efficacemente gli incidenti di sicurezza informatica riguardanti i CIS;

(6) avvia una procedura di emergenza in caso di emergenze in materia di sicurezza informatica;

(7) detiene la responsabilità finale per la sicurezza informatica, comprese le responsabilità del proprietario del sistema e del proprietario dei dati;

(8) sostiene i rischi legati ai loro CIS e alle loro serie di dati;

(9) risolve eventuali divergenze tra i proprietari dei dati e i proprietari dei sistemi e, in caso di disaccordo persistente, porta la questione dinanzi all'ISSB per trovare una soluzione;

(10) assicura che i piani e le misure di sicurezza informatica siano attuati e che i rischi siano adeguatamente coperti.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 9

Proprietari dei sistemi

1. Il proprietario del sistema è responsabile della sicurezza informatica del CSI e riferisce al capo del servizio della Commissione.

2. In relazione alla sicurezza informatica, il proprietario del sistema:

a) assicura la conformità del CIS alla politica in materia di sicurezza informatica;

b) assicura che il CIS sia accuratamente registrato nel relativo inventario;

c) valuta i rischi per la sicurezza informatica e determina le esigenze in materia di sicurezza informatica per ogni CIS, in collaborazione con i proprietari dei dati e in consultazione con la direzione generale dell'Informatica;

d) elabora un piano di sicurezza che comprende, se del caso, precisazioni sui rischi stimati e eventuali ulteriori misure di sicurezza necessarie;

e) attua misure di sicurezza informatica adeguate, proporzionali ai rischi individuati, e segue le raccomandazioni approvate dall'ISSB;

f) individua le dipendenze in relazione ad altri CIS o servizi informatici condivisi e attua adeguate misure di sicurezza sulla base dei livelli di sicurezza proposti dai CIS o dai servizi informatici condivisi in questione:

g) gestisce e monitora i rischi in materia di sicurezza informatica;

h) riferisce periodicamente al capo del servizio della Commissione sul profilo di rischio per la sicurezza informatica dei CIS e riferisce alla direzione generale dell'Informatica in merito ai rischi connessi, alle attività di gestione dei rischi e alle misure di sicurezza adottate;

i) consulta il LISO dei servizi competenti della Commissione in merito agli aspetti della sicurezza informatica;

j) pubblica istruzioni per gli utenti sull'uso del CIS e dei dati associati nonché sulle responsabilità degli utenti relative al CIS;

k) chiede l'autorizzazione della direzione generale Risorse umane e sicurezza, in qualità di autorità Crypto, per qualsiasi CIS che utilizzi le tecnologie di crittografia;

l) consulta l'autorità di sicurezza della Commissione in anticipo in merito a qualsiasi sistema per il trattamento delle informazioni classificate dell'UE;

m) garantisce che copie di backup di tutte le chiavi di decriptazione siano conservate in un conto bloccato di garanzia. Il recupero dei dati crittati è effettuato solo se autorizzato in conformità del quadro definito dalla direzione generale Risorse umane e sicurezza;

n) rispetta le istruzioni dei controllori dei dati pertinenti in materia di protezione dei dati personali e di applicazione delle norme sulla protezione dei dati in materia di sicurezza del trattamento;

o) informa la direzione generale dell'Informatica delle eccezioni alla politica di sicurezza informatica della Commissione, allegando le giustificazioni pertinenti;

p) trasmette eventuali controversie non risolvibili tra il proprietario dei dati e il proprietario del sistema al capo del servizio della Commissione, comunica gli incidenti di sicurezza informatica alle pertinenti parti interessate in modo tempestivo, in funzione delle circostanze, a seconda della gravità dei casi di cui all'articolo 15;

q) per i sistemi esternalizzati, assicura che adeguati sistemi di sicurezza informatica siano inclusi nei contratti di esternalizzazione e che gli incidenti di sicurezza informatica che si verificano nei CIS esternalizzati siano segnalati ai sensi dell'articolo 15;

r) per i CIS che forniscono servizi informatici condivisi, garantisce che un determinato livello di sicurezza, chiaramente documentato, sia attuato e che misure di sicurezza siano attuate per i CIS in questione al fine di raggiungere il livello di sicurezza.

3. I proprietari dei sistemi possono formalmente delegare alcuni o tutti i loro compiti in materia di sicurezza informatica, ma restano responsabili della sicurezza informatica dei loro CIS.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 10

Proprietari dei dati

1. Il proprietario dei dati è responsabile della sicurezza informatica di un set di dati specifico nei confronti del capo del servizio della Commissione e risponde direttamente per la riservatezza, l'integrità e la disponibilità del set di dati.

2. In relazione ai set di dati, il proprietario dei dati:

a) garantisce che tutti i set di dati sotto la sua responsabilità siano adeguatamente classificati in conformità alle decisioni (UE, Euratom) 2015/443 e 2015/444;

b) definisce le esigenze di sicurezza delle informazioni e ne informa i rispettivi proprietari dei sistemi;

c) partecipa alla valutazione del rischio per il CIS;

d) trasmette eventuali controversie non risolvibili tra il proprietario dei dati e il proprietario del sistema al capo del servizio della Commissione;

e) comunica gli incidenti di sicurezza informatica conformemente all'articolo 15.

3. I proprietari dei dati possono formalmente delegare alcuni o tutti i loro compiti in materia di sicurezza informatica, ma restano responsabili di quanto specificato al presente articolo.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 11

Responsabili della sicurezza informatica a livello locale (LISO)

In relazione alla sicurezza informatica, il LISO:

a) identifica in modo proattivo e informa i proprietari dei sistemi, i proprietari dei dati e gli altri ruoli con responsabilità in materia di sicurezza informatica all'interno dei servizi della Commissione in materia di sicurezza informatica;

b) collabora in merito a temi che riguardano la sicurezza informatica nei servizi della Commissione con la direzione generale dell'Informatica nell'ambito della rete LISO;

c) partecipa alle riunioni periodiche dei LISO;

d) mantiene una visione globale del processo di gestione del rischio per la sicurezza delle informazioni e dell'elaborazione e attuazione di piani di sicurezza dei sistemi informatici;

e) fornisce consulenze ai proprietari dei dati, ai proprietari dei sistemi e ai capi dei servizi della Commissione su temi che riguardano la sicurezza informatica;

f) collabora con la direzione generale dell'Informatica per diffondere le buone pratiche in materia di sicurezza informatica e propone programmi specifici di sensibilizzazione e formazione;

g) riferisce sulla sicurezza informatica e segnala le carenze e i miglioramenti al capo dei servizi della Commissione.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 12

Utenti

1. In relazione alla sicurezza informatica, gli utenti:

a) rispettano la politica in materia di sicurezza informatica e le istruzioni impartite dal proprietario del sistema sull'uso di ciascun CIS;

b) comunicano gli incidenti di sicurezza informatica conformemente all'articolo 15.

2. L'utilizzo dei CIS della Commissione in violazione della politica in materia di sicurezza informatica o delle istruzioni impartite dal proprietario del sistema può dar luogo a procedimenti disciplinari.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

CAPO 3

REQUISITI E OBBLIGHI DI SICUREZZA

Articolo 13

Attuazione della presente decisione

1. L'adozione delle norme di attuazione relative all'articolo 6, e delle relative norme e orientamenti, sarà oggetto di una decisione di autorizzazione della Commissione a favore del membro della Commissione responsabile delle questioni di sicurezza.

2. L'adozione delle norme di attuazione relative alla presente decisione, e delle relative norme e degli orientamenti in materia di sicurezza informatica, sarà oggetto di una decisione di autorizzazione della Commissione a favore del membro della Commissione responsabile dell'informatica.

3. L'ISSB approva le norme di attuazione, le norme e gli orientamenti di cui ai paragrafi 1 e 2 prima della loro adozione.

Articolo 14

Obbligo di rispettare le disposizioni

1. È obbligatorio rispettare le disposizioni delineate nella politica in materia di sicurezza informatica e le relative norme.

2. L'inosservanza delle disposizioni di sicurezza informatica e delle relative norme è passibile di azione disciplinare conformemente ai trattati, allo statuto dei funzionari e all'RAA, di sanzioni contrattuali e/o di azione legale nell'ambito delle disposizioni normative e regolamentari nazionali.

3. La direzione generale dell'Informatica è informata di eventuali eccezioni alla politica in materia di sicurezza informatica.

4. Nel caso in cui l'ISSB decida che esiste un rischio inaccettabile per un CIS della Commissione, la direzione generale dell'Informatica in collaborazione con il proprietario del sistema sottopone misure di mitigazione all'approvazione dell'ISSB. Tali misure possono tra l'altro comprendere il rafforzamento del monitoraggio e della rendicontazione, limitazioni del servizio e l'interruzione delle forniture.

5. L'ISSB impone l'attuazione di misure di mitigazione ove necessario. Può anche raccomandare al direttore generale della direzione generale Risorse umane e sicurezza di aprire un'indagine amministrativa. La direzione generale dell'Informatica riferisce all'ISSB in merito a ogni situazione in cui vengono imposte misure di attenuazione.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

Articolo 15

Trattamento degli incidenti di sicurezza informatica

1. La direzione generale dell'Informatica è il principale responsabile della fornitura di capacità di risposta agli incidenti di sicurezza informatica operativa all'interno della Commissione europea.

2. La direzione generale Risorse umane e sicurezza, in quanto soggetto che coadiuva la risposta agli incidenti di sicurezza informatica:

a) ha il diritto di accedere a informazioni sintetiche su ogni incidente e alla documentazione completa su richiesta;

b) partecipa a gruppi di gestione delle crisi a seguito di incidenti di sicurezza informatica e alle procedure di emergenza in caso di incidente informatico;

c) è incaricata delle relazioni con i servizi di contrasto e i servizi segreti;

d) svolge analisi forensi riguardanti la sicurezza informatica, conformemente all'articolo 11 della decisione (UE, Euratom) 2015/443;

e) decide in merito alla necessità di avviare un'indagine formale;

f) informa la direzione generale dell'Informatica di eventuali incidenti di sicurezza informatica che potrebbero presentare un rischio per altri CIS.

3. Tra la direzione generale dell'Informatica e la direzione generale Risorse umane e sicurezza si tengono comunicazioni periodiche per scambiare informazioni e coordinare la gestione degli incidenti di sicurezza e, in particolare, di quelli che potrebbero richiedere un'indagine formale.

4. È possibile avvalersi dei servizi di coordinamento degli incidenti della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee («CERT-UE») per coadiuvare, se del caso, la procedura di trattamento degli incidenti e condividere le conoscenze con altre istituzioni e agenzie dell'UE che potrebbero essere coinvolte.

5. I proprietari dei sistemi coinvolti in un incidente di sicurezza informatica:

a) notificano immediatamente al capo dei servizi della Commissione, alla direzione generale dell'Informatica, alla direzione generale Risorse umane, al LISO e, se del caso, al proprietario dei dati gli incidenti gravi di sicurezza informatica, in particolare quelli riguardanti la violazione della riservatezza dei dati;

b) cooperano e seguono le istruzioni delle autorità competenti della Commissione in materia di comunicazione degli incidenti, risposta e ripristino.

6. Gli utenti comunicano tempestivamente all'helpdesk competente tutti gli incidenti, concreti o sospetti, di sicurezza informatica.

7. I proprietari dei dati comunicano tempestivamente alla squadra di pronto intervento informatico competente tutti gli incidenti, concreti o sospetti, di sicurezza informatica.

8. La direzione generale dell'Informatica, con il sostegno degli altri soggetti coinvolti, è responsabile del trattamento di qualsiasi incidente di sicurezza informatica rilevato in relazione ai CIS della Commissione che non siano sistemi esternalizzati.

9. La direzione generale dell'Informatica informa i servizi interessati della Commissione in merito a incidenti di sicurezza informatica, i LISO pertinenti e, se del caso, il CERT-UE sulla base del principio della necessità di sapere.

10. La direzione generale dell'Informatica trasmette periodicamente all'ISSB una relazione sugli indicenti gravi di sicurezza informatica che interessano i CIS della Commissione.

11. Su richiesta, il LISO pertinente ha accesso alla documentazione relativa all'incidente di sicurezza informatica riguardante il CIS del servizio della Commissione.

12. In caso di grave incidente di sicurezza informatica, la direzione generale dell'Informatica è il punto di contatto per la gestione delle situazioni di crisi e coordina i gruppi di gestione delle crisi a seguito di incidenti di sicurezza informatica.

13. In caso di emergenza, il direttore generale della direzione generale dell'Informatica può decidere di avviare una procedura di emergenza in materia di sicurezza informatica. La direzione generale dell'Informatica elabora procedure di emergenza che devono essere approvate dall'ISSB.

14. La direzione generale dell'Informatica trasmette all'ISSB e ai capi dei servizi della Commissione interessati una relazione sull'esecuzione delle procedure di emergenza.

I processi relativi a queste responsabilità e attività sono ulteriormente dettagliati nelle norme di attuazione.

CAPO 4

DISPOSIZIONI FINALI

Articolo 16

Trasparenza

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

Articolo 17

Relazione con altri atti

Le disposizioni della presente decisione lasciano impregiudicati la decisione (UE, Euratom) 2015/443, la decisione (UE, Euratom) 2015/444, il regolamento (CE) n. 45/2001, il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([1]), la decisione (CE, CECA, Euratom) 2002/47 ([2]), il regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio ([3]), la decisione 1999/352/CE, CECA, Euratom.

Articolo 18

Abrogazione e disposizioni transitorie

La decisione C(2006) 3602 del 16 agosto 2006 è abrogata.

Le norme di attuazione e le norme di sicurezza informatica adottate a norma dell'articolo 10 della decisione C(2006) 3602 rimangono in vigore nella misura in cui non siano in contrasto con la presente decisione, fino a quando non saranno sostituite dalle norme di attuazione e dalle norme che devono essere adottate conformemente all'articolo 13 della presente decisione. Ogni riferimento all'articolo 10 della decisione C(2006)3602 deve essere letto come un riferimento all'articolo 13 della presente decisione.

Articolo 19

Entrata in vigore

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

Fatto a Bruxelles, il 10 gennaio 2017

Per la Commissione
Il presidente
Jean-Claude JUNCKER

([1]) 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).
([2]) Decisione (CE, CECA, Euratom) 2002/47 della Commissione, del 23 gennaio 2002, recante modificazione del suo regolamento interno (GU L 21 del 24.1.2002, pag. 23).
([3]) Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).