DECISIONE (UE, Euratom) 2018/559 DELLA COMMISSIONE

del 6 aprile 2018

che stabilisce le norme di attuazione dell'articolo 6 della decisione (EU, Euratom) 2017/46 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,

vista la decisione (UE, Euratom) 2017/46 della Commissione del 10 gennaio 2017 sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea ([1]), in particolare l'articolo 6,

considerando quanto segue:

(1) A seguito dell'adozione della decisione (UE, Euratom) 2017/46 è necessario che la Commissione riesamini, aggiorni e consolidi le norme di attuazione della decisione C(2006)3602 della Commissione sulla sicurezza dei sistemi di comunicazione e informazione utilizzati dalla Commissione, ora abrogata.

(2) Al membro della Commissione responsabile della Sicurezza è conferito, nel pieno rispetto delle norme e procedure interne, il potere di stabilire norme di attuazione in conformità all'articolo 13 della decisione (UE, Euratom) 2017/46 ([2]).

(3) È opportuno, pertanto, abrogare le norme di attuazione della decisione C(2006)3602,

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. L'oggetto e l'ambito di applicazione della presente decisione figurano all'articolo 1 della decisione (UE, Euratom) 2017/46.

2. Le disposizioni della presente decisione si applicano a tutti i sistemi di comunicazione e informazione (CIS). Tuttavia, le responsabilità definite nella presente decisione non si applicano ai CIS che elaborano le informazioni classificate UE. Le pertinenti responsabilità per questi sistemi sono determinate dal proprietario del sistema e dall'autorità di sicurezza della Commissione, conformemente alla decisione (UE, Euratom) 2015/444 ([3]).

3. Il capo 2 della presente decisione presenta il quadro dell'attuazione pratica dell'organizzazione e delle responsabilità relative alla sicurezza informatica. Il capo 3 della presente decisione presenta il quadro dei processi attinenti all'articolo 6 della decisione (UE, Euratom) 2017/46 della Commissione.

Articolo 2

Definizioni

Alla presente decisione si applicano le definizioni di cui all'articolo 2 della decisione (UE, Euratom) 2017/46. Ai fini della presente decisione si applicano inoltre le seguenti definizioni:

1. «autorità di approvazione degli apparati crittografici» (CAA), funzione assunta dall'autorità di sicurezza della Commissione posta sotto l'autorità del direttore generale delle Risorse umane e della sicurezza;

([1]) GU L 6 dell'11.1.2017, pag. 40.
([2]) Decisione C(2017) 7428 della Commissione dell'8 novembre 2017 che conferisce il potere di adottare norme di attuazione, norme e orientamenti relativi alla sicurezza dei sistemi di comunicazione e informazione utilizzati dalla Commissione europea.
([3]) 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).

2. «connessione a una rete esterna», qualsiasi connessione per le comunicazioni elettroniche tra la rete interna della Commissione e qualsiasi altra rete, compreso Internet. Da questa definizione sono escluse le reti di terzi che, da contratto, sono fornite per essere integrate nella rete interna della Commissione;

3. «deposito della chiave presso terzi (key escrow)», procedura per l'archiviazione di copie delle chiavi crittografiche presso una o più parti separate, che garantisce la separazione delle funzioni, per consentirne il recupero qualora venga persa la copia operativa. Le chiavi possono essere divise in due o più parti, ciascuna delle quali è depositata presso una parte diversa per garantire che nessuna delle parti possegga da sola l'intera chiave;

4. «RASCI», acronimo per la distribuzione delle responsabilità basata sui seguenti indicatori di attribuzione:

   a) «responsabile» (responsible, R): che ha l'obbligo di agire e prendere decisioni per conseguire i risultati richiesti;

   b) «tenuto a rispondere» (accountable, A): che deve rendere conto di azioni, decisioni e prestazioni;

   c) «tenuto a fornire un sostegno» (supports, S): che ha l'obbligo di cooperare con la persona responsabile di eseguire il compito;

   d) «consultato» (consulted, C): che è consultato per fornire consigli o pareri;

   e) «informato» (informed, I): che è tenuto al corrente delle pertinenti informazioni.

CAPO 2

ORGANIZZAZIONE E RESPONSABILITÀ

Articolo 3

Ruoli e responsabilità

I ruoli e le responsabilità relativi agli articoli da 4 a 8 della presente decisione sono definiti nell'allegato in conformità al modello RASCI.

Articolo 4

Allineamento alla politica in materia di sicurezza informatica della Commissione

1. La direzione generale Risorse umane e sicurezza riesamina la politica di sicurezza informatica della Commissione e le norme e gli orientamenti relativi, per garantirne la conformità alle politiche generali di sicurezza della Commissione, in particolare la decisione (UE, Euratom) 2015/443 della Commissione ([1]) e la decisione (UE, Euratom) 2015/444.

2. Su richiesta di altri servizi della Commissione la direzione generale Risorse umane e sicurezza può riesaminarne le politiche di sicurezza informatica o altra documentazione sulla sicurezza informatica per assicurarne la conformità alla politica di sicurezza informatica della Commissione. Il capo del servizio della Commissione interessato si assicura che siano rimosse le eventuali incoerenze.

3. In quanto responsabile per la sicurezza delle informazioni, la direzione generale Risorse umane e sicurezza coopera con la direzione generale dell'Informatica per garantire che i processi di sicurezza informatica tengano pienamente conto della classificazione e dei principi di sicurezza di cui alla decisione (UE, Euratom) 2015/443, in particolare gli articoli 3 e 9.

CAPO 3

PROCESSI DI SICUREZZA INFORMATICA

Articolo 5

Tecnologie di crittografia

1. L'uso di tecnologie di crittografia per la protezione delle informazioni classificate UE (ICUE) è conforme alla decisione (UE, Euratom) 2015/444.

2. Le decisioni relative all'uso delle tecnologie di crittografia per la protezione dei dati non ICUE sono adottate dal proprietario del sistema di ciascun CIS, tenendo conto sia dei rischi che si vogliono ridurre grazie alla crittografia sia dei rischi che l'uso della crittografia comporta.

3. L'approvazione preventiva della CAA è richiesta per tutti gli usi delle tecnologie di crittografia, a meno che la crittografia sia utilizzata esclusivamente per proteggere la riservatezza dei dati non ICUE in transito e utilizzi protocolli standard per le comunicazioni di rete.

([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).

4. Con l'eccezione di cui al paragrafo 3, i servizi della Commissione si assicurano che copie di backup di tutte le chiavi di decriptazione siano depositate presso terzi allo scopo di recuperare le informazioni memorizzate nel caso in cui la chiave di decriptazione non sia disponibile. Il recupero dei dati criptati utilizzando i backup delle chiavi di decriptazione viene effettuato solo previa autorizzazione in conformità alla norma definita dalla CAA.

5. Le domande di approvazione dell'uso delle tecnologie di crittografia sono formalmente documentate e includono tutte le informazioni sul CIS e i dati da proteggere, le tecnologie da usare e le relative procedure operative di sicurezza. Le domande di approvazione sono firmate dal proprietario del sistema.

6. Le domande di approvazione dell'uso delle tecnologie di crittografia sono valutate dalla CAA in conformità alle norme e ai requisiti pubblicati.

Articolo 6

Ispezioni sulla sicurezza informatica

1. La direzione generale Risorse umane e sicurezza effettua ispezioni sulla sicurezza informatica per verificare che le misure di sicurezza informatica siano conformi alle politiche di sicurezza informatica della Commissione e accertarsi dell'integrità di tali misure di controllo.

2. La direzione generale Risorse umane e sicurezza può effettuare un'ispezione sulla sicurezza informatica:

a) di propria iniziativa;

b) su richiesta del comitato direttivo per la sicurezza dell'informazione (ISSB);

c) su richiesta pervenuta da un proprietario del sistema;

d) a seguito di un incidente di sicurezza informatica; oppure

e) qualora sia stato individuato un rischio elevato per un particolare sistema.

3. I proprietari dei dati possono richiedere che sia effettuata un'ispezione sulla sicurezza informatica prima di archiviare le loro informazioni in un CIS.

4. I risultati dell'ispezione sono documentati in una relazione ufficiale inviata al proprietario del sistema, con copia al responsabile della sicurezza informatica a livello locale (LISO), contenente le risultanze e le raccomandazioni per migliorare la conformità del CIS alla politica di sicurezza informatica. La direzione generale Risorse umane e sicurezza riferisce all'ISSB in merito ai principali problemi e alle raccomandazioni formulate.

5. La direzione generale Risorse umane e sicurezza verifica l'attuazione delle raccomandazioni.

6. Laddove opportuno, le ispezioni sulla sicurezza informatica comprendono l'ispezione di servizi, locali e apparecchiature fornite al proprietario del sistema, e riguardano i fornitori di servizi sia interni sia esterni.

Articolo 7

Accesso dalle reti esterne

1. La direzione generale Risorse umane e sicurezza fissa le regole in una norma sull'autorizzazione dell'accesso tra i CIS della Commissione e le reti esterne.

2. Tali regole operano una distinzione tra i diversi tipi di connessioni da reti esterne e stabiliscono appropriate regole di sicurezza per ciascun tipo di connessione, precisando anche se è necessaria la previa autorizzazione dell'autorità competente, come indicato al paragrafo 4.

3. Se necessario, l'autorizzazione viene concessa sulla base di una richiesta e di un processo di approvazione formali. L'approvazione è valida per una durata determinata e deve essere ottenuta prima di attivare la connessione.

4. La direzione generale Risorse umane e sicurezza ha la responsabilità generale di autorizzare le domande, ma può, ai sensi dell'articolo 17, paragrafo 3, della decisione (EU/Euratom) 2015/443, delegare, a propria discrezione, la responsabilità di autorizzare alcuni tipi di connessioni, fatte salve le condizioni di cui al paragrafo 8.

5. L'entità che rilascia l'autorizzazione può imporre requisiti di sicurezza aggiuntivi come prerequisito per l'approvazione al fine di proteggere il CIS e le reti della Commissione dai rischi di accesso non autorizzato e altre violazioni della sicurezza.

6. La direzione generale dell'Informatica è il fornitore abituale di servizi di rete per la Commissione. Ogni altro servizio della Commissione che utilizza una rete non fornita dalla direzione generale dell'Informatica ottiene la previa autorizzazione dell'ISSB. Il servizio della Commissione documenta la giustificazione commerciale alla base della richiesta e dimostra che i controlli sulla rete sono sufficienti per rispettare i requisiti di verifica dei flussi di informazioni in entrata e in uscita.

7. Il proprietario del sistema del CIS stabilisce i requisiti di sicurezza per l'accesso esterno a tale CIS e garantisce, con il sostegno del LISO, l'attuazione di adeguate misure per proteggerne la sicurezza.

8. Le misure di sicurezza attuate per le connessioni da rete esterna si basano sui principi della necessità di conoscere e del privilegio minimo, in virtù dei quali i singoli ricevono esclusivamente le informazioni e i diritti di accesso necessari all'espletamento dei loro incarichi ufficiali per la Commissione.

9. Tutte le connessioni da rete esterna sono filtrate e monitorate per individuare potenziali violazioni della sicurezza.

10. Quando le connessioni sono stabilite per consentire l'esternalizzazione di un CIS, l'autorizzazione è subordinata al positivo completamento della procedura di cui all'articolo 8.

Articolo 8

Esternalizzazione dei CIS

1. Ai fini della presente decisione un CIS si considera esternalizzato quando viene fornito sulla base di un contratto con un appaltatore terzo in virtù del quale il CIS è ospitato in locali non appartenenti alla Commissione. L'esternalizzazione riguarda uno o più CIS o altri servizi informatici e centri dati situati in locali non appartenenti alla Commissione e la gestione di dataset della Commissione da parte di servizi esterni.

2. Nell'esternalizzare un CIS si tiene conto della sensibilità o della classificazione delle informazioni trattate, secondo le seguenti modalità:

a) i CIS che elaborano le ICUE sono accreditati in conformità alla decisione (UE, Euratom) 2015/444, previa consultazione dell'autorità di accreditamento in materia di sicurezza della Commissione. I sistemi che elaborano le ICUE non sono esternalizzati;

b) il proprietario del sistema del CIS che elabora informazioni non ICUE applica misure proporzionate per soddisfare le esigenze di sicurezza in conformità ai pertinenti obblighi giuridici o alla sensibilità delle informazioni, tenendo conto dei rischi dell'esternalizzazione. La direzione generale Risorse umane e sicurezza può imporre requisiti supplementari;

c) i progetti di sviluppo esternalizzati tengono conto della sensibilità del codice sviluppato e di eventuali dati delle prove utilizzati nella fase di sviluppo.

3. In aggiunta ai principi di cui all'articolo 3 della decisione (UE, Euratom) 2017/46, ai CIS esternalizzati si applicano i seguenti principi:

a) gli accordi di esternalizzazione sono formulati in modo tale da evitare la dipendenza da specifici fornitori;

b) le disposizioni di sicurezza relative all'esternalizzazione riducono al minimo le possibilità che il personale di terzi abbia accesso alle informazioni della Commissione o le modifichi;

c) il personale che ha accesso al CIS esternalizzato sottoscrive un accordo di riservatezza;

d) l'esternalizzazione del CIS viene registrata nell'inventario dei CIS.

4. Il proprietario del sistema, con la partecipazione del proprietario dei dati:

a) verifica e documenta il rischi connessi con l'esternalizzazione;

b) stabilisce i pertinenti requisiti di sicurezza;

c) si consulta con i proprietari dei sistemi di tutti gli altri CIS connessi per garantire che siano inclusi i loro requisiti di sicurezza;

d) si assicura che nel contratto di esternalizzazione siano inclusi adeguati requisiti e diritti di sicurezza;

e) rispetta tutti gli altri requisiti previsti dalla procedura dettagliata di cui al paragrafo 8.

Questi interventi devono essere completati prima della firma del contratto o altro accordo di esternalizzazione di uno o più CIS.

5. I proprietari dei sistemi gestiscono i rischi connessi con l'esternalizzazione durante la durata di vita del CIS al fine di ottemperare ai requisiti di sicurezza definiti.

6. I proprietari dei sistemi si assicurano che gli appaltatori terzi siano tenuti a notificare immediatamente alla Commissione tutti gli incidenti di sicurezza informatica che interessano un CIS della Commissione esternalizzato.

7. Il proprietario del sistema è responsabile di garantire la conformità del CIS, del contratto di esternalizzazione e delle disposizioni di sicurezza alle norme della Commissione in materia di sicurezza delle informazioni e sicurezza informatica.

8. La direzione generale Risorse umane e sicurezza stabilisce una norma dettagliata relativa alle responsabilità e attività di cui ai punti da 1) a 7), in conformità all'articolo 10.

CAPO 4

DISPOSIZIONI VARIE E FINALI

Articolo 9

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 10

Norme

1. Laddove necessario, le disposizioni della presente decisione sono ulteriormente specificate in norme e/o orientamenti in conformità alla decisione (UE, Euratom) 2017/46 e alla decisione C(2017)7428.. Le norme e gli orientamenti in materia di sicurezza informatica forniscono ulteriori dettagli sulle presenti norme di attuazione e sulla decisione (UE, Euratom) 2017/46 in relazione ad ambiti di sicurezza specifici in conformità alla norma ISO 27001:2013, allegato A. Tali norme e orientamenti si basano sulle migliori pratiche del settore e sono selezionati in modo da essere compatibili con l'ambiente informatico della Commissione.

2. Se necessario, e in conformità alla norma ISO 27001:2013, allegato A, sono elaborate norme attinenti agli ambiti di seguito specificati:

1) organizzazione della sicurezza informatica;

2) sicurezza delle risorse umane;

3) gestione di attività;

4) controllo dell'accesso;

5) crittografia;

6) sicurezza fisica e dell'ambiente;

7) sicurezza operativa;

8) sicurezza delle comunicazioni;

9) acquisizione, sviluppo e manutenzione di sistemi;

10) relazioni con i fornitori;

11) gestione degli incidenti relativi alla sicurezza informatica;

12) aspetti della sicurezza informatica attinenti alla gestione della continuità operativa;

13) conformità.

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

4. Sono abrogate le norme di attuazione della decisione C(2006)3602 attinenti all'ambito di applicazione della presente decisione.

5. Le norme e gli orientamenti adottati a norma della decisione C(2006)3602 del 16 agosto 2006 rimangono in vigore nella misura in cui non siano in contrasto con le presenti norme di attuazione e fino a quando siano abrogati o sostituiti da norme o orientamenti da adottare ai sensi dell'articolo 13 della decisione (UE, Euratom) 2017/46.

Articolo 11

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 6 aprile 2018

Per la Commissione,
a nome del presidente
Günther OETTINGER
Membro della Commissione

ALLEGATO

RUOLI E RESPONSABILITÀ (RASCI)

Il modello RASCI assegna i ruoli alle entità utilizzando le seguenti abbreviazioni:

a) R — Responsabile (Responsible)

b) A — Tenuto a rispondere (Accountable)

c) S — Tenuto a fornire un sostegno (Supporting)

d) C — Consultato (Consulted)

e) I — Informato (Informed)

Ruolo / Processo	ISSB	HR (DS)	Commissione Servizi	Proprietario del sistema	Proprietario dei dati	LISO	DIGIT	Appaltatori
Allineamento alla politica in materia di sicurezza informatica della Commissione		**R/A**	**S**				**S**	
Tecnologie di crittografia		**C**	**A**	**R**	**I**	**C**		
Ispezioni di sicurezza informatica	**I**	**A/R**		**S**	**I**	**I**	**S**	
Accesso dalle reti esterne	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Esternalizzazione dei CIS		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] L'ISSB è consultato in relazione al funzionamento delle reti interne da qualsiasi servizio della Commissione che non sia la direzione generale dell'Informatica.

[2] Responsabile è il proprietario del sistema del CIS che viene esternalizzato, mentre è consultato il proprietario del sistema di qualsiasi altro CIS interconnesso con il CIS esternalizzato.