DECISIÓN (UE, Euratom) 2018/559 DE LA COMISIÓN

de 6 de abril de 2018

relativa al establecimiento de disposiciones de aplicación para el artículo 6 de la Decisión (UE, Euratom) 2017/46 sobre la seguridad de los sistemas de información y comunicación de la Comisión Europea

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 249,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica,

Vista la Decisión (UE, Euratom) 2017/46 de la Comisión, de 10 de enero de 2017, sobre la seguridad de los sistemas de información y comunicación de la Comisión Europea ([1]), y en particular su artículo 6,

Considerando lo siguiente:

(1) La adopción de la Decisión (UE, Euratom) 2017/46 hace necesario que la Comisión revise, actualice y consolide las disposiciones de aplicación vinculadas a la Decisión derogada C(2006) 3602 de la Comisión sobre la seguridad de los sistemas de comunicación e información utilizados por la Comisión.

(2) El miembro de la Comisión responsable de los asuntos de seguridad, de plena conformidad con el reglamento interno, ha sido habilitado para establecer disposiciones de aplicación de conformidad con el artículo 13 de la Decisión (UE, Euratom) 2017/46 ([2]).

(3) Las disposiciones de aplicación de la Decisión C(2006) 3602 deben, por tanto, derogarse.

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. El objeto y el ámbito de aplicación de la presente Decisión están establecidos en el artículo 1 de la Decisión (UE, Euratom) 2017/46.

2. Las disposiciones de la presente Decisión se aplican a todos los sistemas de información y comunicaciones (SIC). No obstante, las responsabilidades definidas en la presente Decisión no se aplicarán a los SIC que manejen información clasificada de la UE. Las responsabilidades correspondientes a estos sistemas serán determinadas por el propietario del sistema y la autoridad de seguridad de la Comisión de conformidad con la Decisión (UE, Euratom) 2015/444 de la Comisión ([3]).

3. En el capítulo 2 de la presente Decisión se expone resumidamente la aplicación práctica de la organización y las responsabilidades por lo que respecta a la seguridad informática. En su capítulo 3 se describen los procesos relacionados con el artículo 6 de la Decisión (UE, Euratom) 2017/46.

Artículo 2

Definiciones

Las definiciones del artículo 2 de la Decisión (UE, Euratom) 2017/46 se aplican a la presente Decisión. A efectos de la presente Decisión, se entenderá asimismo por:

1) «autoridad de certificación criptológica (ACC)»: función asumida por la autoridad de seguridad de la Comisión, que depende del director general de Recursos Humanos y Seguridad;

([1]) DO L 6 de 11.1.2017, p. 40.
([2]) Decisión C(2017) 7428 final de la Comisión, de 8 de noviembre de 2017, concediendo una habilitación para adoptar las disposiciones de aplicación, normas y directrices relacionadas con la seguridad de los sistemas de información y comunicaciones en la Comisión Europea.
([3]) Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

2) «conexión a red externa»: cualquier conexión de comunicaciones electrónicas entre la red interna de la Comisión y cualquier otra red, incluido internet; esta definición excluye las redes de terceros que se suministran con arreglo a un contrato para que formen parte de la red interna de la Comisión;

3) «depósito de claves»: procedimiento para el almacenamiento de copias de claves criptográficas en una o más partes diferentes, garantizando la separación de tareas, para permitir su recuperación en caso de que se pierda la copia operativa; las claves pueden dividirse en dos o más fracciones, cada una de ellas alojada en una parte diferente para garantizar que ninguna parte posea por sí sola la clave completa;

4) «RASCI»: abreviatura en inglés correspondiente a una distribución de responsabilidades basada en los siguientes indicadores de atribuciones:

   a) «ser responsable» (R): estar obligado a actuar y tomar decisiones con el fin de lograr los resultados requeridos;

   b) «rendir cuentas» (A): tener que responder acerca de las acciones, las decisiones y el rendimiento;

   c) «prestar apoyo» (S): tener la obligación de trabajar con la persona responsable de llevar a cabo la tarea;

   d) «ser consultado» (C): recibir solicitudes de asesoramiento u opinión;

   e) «estar informado» (I): disponer de la información pertinente actualizada en todo momento.

CAPÍTULO 2

ORGANIZACIÓN Y RESPONSABILIDADES

Artículo 3

Funciones y responsabilidades

Las funciones y responsabilidades relacionadas con los artículos 4 a 8 de la presente Decisión se definen en el anexo de conformidad con el modelo RASCI.

Artículo 4

Conformidad con las políticas de seguridad de la información de la Comisión

1. La Dirección General de Recursos Humanos y Seguridad revisará la política de seguridad informática de la Comisión y las normas y directrices conexas para garantizar que se ajusten a las políticas generales de seguridad de la Comisión, y en particular a la Decisión (UE, Euratom) 2015/443 de la Comisión ([1]) y la Decisión (UE, Euratom) 2015/444.

2. A petición de otros servicios de la Comisión, la Dirección General de Recursos Humanos y Seguridad podría revisar sus políticas de seguridad informática u otra documentación de seguridad informática para garantizar su coherencia con la política de seguridad de la información de la Comisión. El jefe del servicio de la Comisión de que se trate se asegurará de que se subsanen todas las incoherencias.

3. Como parte de su responsabilidad por la seguridad de la información, la Dirección General de Recursos Humanos y Seguridad cooperará con la Dirección General de Informática para garantizar que los procesos de seguridad informática tienen plenamente en cuenta la clasificación y los principios de seguridad establecidos en la Decisión (UE, Euratom) 2015/443, y en particular sus artículos 3 y 9.

CAPÍTULO 3

PROCESOS DE SEGURIDAD INFORMÁTICA

Artículo 5

Tecnologías de cifrado

1. El uso de tecnologías de cifrado para la protección de la información clasificada de la UE (ICUE) deberá cumplir lo dispuesto en la Decisión (UE, Euratom) 2015/444.

2. Las decisiones sobre el uso de tecnologías de cifrado para la protección de datos que no sean ICUE será adoptada por el propietario del sistema de cada SIC, teniendo en cuenta tanto los riesgos que se quiere mitigar mediante el cifrado como los riesgos que este introduce.

3. Se requiere la aprobación previa de la ACC para todos los usos de tecnologías de cifrado, a menos que el cifrado se utilice únicamente para proteger la confidencialidad de datos en tránsito que no sean ICUE y utilice protocolos estándar de comunicaciones en red.

([1]) Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (DO L 72 de 17.3.2015, p. 41).

4. Con la excepción enunciada en el apartado 3 del presente artículo, los servicios de la Comisión se asegurarán de que se almacenan en un depósito de claves copias de seguridad de cualquier clave de descifrado, con el fin de recuperar los datos almacenados en caso de que no esté disponible la clave de descifrado. La recuperación de datos cifrados utilizando copias de seguridad de claves de descifrado únicamente podrá realizarse cuando se haya autorizado en línea con la norma definida por la ACC.

5. Las solicitudes para la aprobación del uso de tecnologías de cifrado deberán documentarse oficialmente e incluir detalles del SIC y de los datos que se trata de proteger, las tecnologías que se quiere utilizar y los procedimientos operativos de seguridad conexos. Estas solicitudes de aprobación deberán ser firmadas por el propietario del sistema.

6. Las solicitudes de aprobación para el uso de tecnologías de cifrado serán evaluadas por la ACC de conformidad con las normas y los requisitos publicados.

Artículo 6

Inspecciones de seguridad informática

1. La Dirección General de Recursos Humanos y Seguridad llevará a cabo inspecciones de seguridad informática a fin de verificar si las medidas de seguridad informática cumplen las políticas de seguridad informática de la Comisión y de comprobar la integridad de estas medidas de control.

2. La Dirección General de Recursos Humanos y Seguridad podrá realizar una inspección de seguridad informática:

a) por iniciativa propia;

b) a instancias del Consejo Director de Seguridad de la Información (ISSB);

c) en respuesta a una solicitud recibida del propietario de un sistema;

d) a raíz de un incidente de seguridad, o

e) tras haberse detectado un alto riesgo para un sistema concreto.

3. Los propietarios de los datos pueden solicitar una inspección de seguridad informática antes de almacenar su información en un SIC.

4. Los resultados de las inspecciones se documentarán al propietario del sistema en un informe oficial, con copia al responsable local de seguridad informática (LISO), que incluirá conclusiones y recomendaciones para mejorar el cumplimiento de la política de seguridad informática por el SIC. La Dirección General de Recursos Humanos y Seguridad comunicará las cuestiones y las recomendaciones significativas al ISSB.

5. La Dirección General de Recursos Humanos y Seguridad supervisará la aplicación de las recomendaciones.

6. Cuando proceda, las inspecciones de seguridad informática incluirán la inspección de los servicios, los locales y el equipo proporcionados al propietario del sistema, incluidos tanto los prestadores de servicios internos como los externos.

Artículo 7

Acceso desde redes externas

1. La Dirección General de Recursos Humanos y Seguridad establecerá las reglas en una norma sobre autorización del acceso entre los SIC de la Comisión y las redes externas.

2. Las reglas distinguirán diferentes tipos de conexiones a redes externas y establecerán reglas de seguridad apropiadas para cada tipo de conexión, que incluirán la especificación de si se requiere para la conexión una autorización previa de la autoridad pertinente, según lo dispuesto en el apartado 4 del presente artículo.

3. Si se requiere una autorización, esta se expedirá previa presentación de una solicitud formal y con arreglo a un proceso de aprobación. La aprobación será válida por un período de duración definida y deberá obtenerse antes de que se active la conexión.

4. La Dirección General de Recursos Humanos y Seguridad tendrá la responsabilidad general sobre las solicitudes de autorización, pero podrá delegar la responsabilidad de la autorización de algunos tipos de conexión, si así lo decide, de conformidad con el artículo 17, apartado 3, de la Decisión (UE, Euratom) 2015/443 y con sujeción a las condiciones establecidas en el apartado 8.

5. La entidad que expida la autorización podrá imponer requisitos de seguridad adicionales como requisito previo para la aprobación, a fin de proteger los SIC y las redes de la Comisión de los riesgos de acceso no autorizado u otros fallos de seguridad.

6. La Dirección General de Informática es el proveedor ordinario de servicios de red para la Comisión. Cualquier otro servicio de la Comisión que funcione con una red no proporcionada por la Dirección General de Informática deberá obtener primero el acuerdo del ISSB. Dicho servicio de la Comisión documentará la justificación de la solicitud desde el punto de vista de su actividad y demostrará que los controles de la red son suficientes para satisfacer los requisitos de control de los flujos de entrada y salida de información.

7. El propietario del sistema de un SIC determinará los requisitos de seguridad para el acceso exterior a ese SIC y se asegurará de que se aplican las medidas adecuadas para proteger su seguridad, con el apoyo del responsable local de seguridad informática.

8. Las medidas de seguridad aplicadas para las conexiones a redes externas se basarán en los principios de la necesidad de saber y el mínimo privilegio, que garantizan que las personas solo reciben la información y acceden a los derechos que necesitan para el desempeño de sus obligaciones oficiales para la Comisión.

9. Todas las conexiones a redes externas se filtrarán y supervisarán para detectar posibles fallos de seguridad.

10. Cuando se establezcan conexiones para permitir la externalización de un SIC, la autorización estará supeditada a que se haya completado con éxito el procedimiento descrito en el artículo 8.

Artículo 8

Externalización de SIC

1. A efectos de la presente Decisión, se considera que un SIC está externalizado cuando se suministra con arreglo a un contrato con un contratista tercero, en virtud del cual el SIC está alojado en locales ajenos a la Comisión. Esto incluye la subcontratación de uno o múltiples SIC u otros servicios informáticos, centros de datos en locales ajenos a la Comisión, así como la manipulación de series de datos de la Comisión por servicios externos.

2. Al externalizar un SIC se tendrá en cuenta el carácter sensible o clasificado de la información que se maneje, de la siguiente manera:

a) los SIC que manejen ICUE deberán estar acreditados de conformidad con la Decisión (UE, Euratom) 2015/444, y se consultará de antemano a la autoridad de acreditación de seguridad de la Comisión. Los sistemas que manejen ICUE no serán externalizados;

b) el propietario del sistema de un SIC que maneje información que no sea ICUE aplicará medidas proporcionadas para cubrir las necesidades de seguridad con arreglo a las obligaciones jurídicas pertinentes o a la sensibilidad de la información, teniendo en cuenta los riesgos de la externalización. La Dirección General de Recursos Humanos y Seguridad podrá imponer requisitos adicionales;

c) al externalizar proyectos de desarrollo se tendrá en cuenta la sensibilidad del código desarrollado y de los datos de ensayo utilizados durante el desarrollo.

3. Se aplicarán a los SIC externalizados los siguientes principios, además de los establecidos en el artículo 3 de la Decisión (UE, Euratom) 2017/46:

a) los acuerdos de externalización estarán concebidos para evitar la dependencia respecto de proveedores específicos;

b) los acuerdos de seguridad de la externalización reducirán al mínimo las posibilidades de que el personal de terceros acceda a información de la Comisión o la modifique;

c) el personal de terceros que tenga acceso a un SIC externalizado deberá proporcionar acuerdos de confidencialidad;

d) la externalización de un SIC se indicará en el inventario de SIC.

4. El propietario del sistema, con la participación del propietario de los datos:

a) evaluará y documentará los riesgos relacionados con la subcontratación;

b) establecerá los requisitos de seguridad pertinentes;

c) consultará a los propietarios del sistema de todos los demás SIC conectados para asegurarse de que sus requisitos de seguridad estén incluidos;

d) se asegurará de que en el contrato de externalización estén incluidos los requisitos y derechos de seguridad apropiados;

e) cumplirá cualquier otro requisito establecido en el procedimiento detallado indicado en el apartado 8 del presente artículo.

Estas acciones se completarán antes de firmar el contrato u otro acuerdo para la externalización de uno o más SIC.

5. Los propietarios del sistema gestionarán los riesgos relacionados con la externalización durante todo el período de vida del SIC a fin de cumplir los requisitos de seguridad definidos.

6. Los propietarios del sistema garantizarán que los terceros contratistas están obligados a notificar de inmediato a la Comisión todos los incidentes de seguridad informática que afecten a un SIC de la Comisión externalizado.

7. El propietario del sistema es responsable de garantizar que el SIC, el contrato de externalización y los mecanismos de seguridad cumplen las normas de la Comisión en materia de seguridad de la información y seguridad informática.

8. La Dirección General de Recursos Humanos y Seguridad establecerá la norma detallada referente a las responsabilidades y actividades expuestas en los puntos 1) a 7) de conformidad con el artículo 10 siguiente.

CAPÍTULO 4

DISPOSICIONES VARIAS Y FINALES

Artículo 9

Transparencia

La presente Decisión será puesta en conocimiento del personal de la Comisión y de todas las personas a las que se aplique, y se publicará en el *Diario Oficial de la Unión Europea*.

Artículo 10

Normas

1. Las disposiciones de la presente Decisión se detallarán con mayor precisión, cuando sea necesario, en normas o directrices que se adoptarán de conformidad con la Decisión (UE, Euratom) 2017/46 y con la Decisión C(2017) 7428. Las normas y directrices de seguridad informática proporcionarán más detalles sobre estas disposiciones de aplicación y la Decisión (UE, Euratom) 2017/46 para ámbitos de seguridad específicos de conformidad con el anexo A de la norma ISO 27001:2013. Estas normas y directrices se basan en las mejores prácticas de la industria y se han seleccionado por su adaptación al entorno informático de la Comisión.

2. Se elaborarán normas, cuando sea necesario, de conformidad con el anexo A de la norma ISO 27001:2013, en los ámbitos siguientes:

1) organización de la seguridad de la información;

2) seguridad de los recursos humanos;

3) gestión de activos;

4) control de acceso;

5) criptografía;

6) seguridad física y del entorno;

7) seguridad operativa;

8) seguridad de las comunicaciones;

9) adquisición, desarrollo y mantenimiento de sistemas;

10) relaciones con los proveedores;

11) gestión de incidentes de seguridad de la información;

12) aspectos de seguridad de la información relacionados con la gestión de la continuidad de las actividades;

13) cumplimiento.

3. El ISSB deberá aprobar las normas mencionadas en los apartados 1 y 2 del presente artículo antes de su adopción.

4. Se derogan las disposiciones de aplicación vinculadas a la Decisión C(2006) 3602 relacionadas con el ámbito de aplicación de la presente Decisión.

5. Las normas y directrices adoptadas en virtud de la Decisión C(2006) 3602 de 16 de agosto de 2006 seguirán en vigor, siempre que no entren en conflicto con estas disposiciones de aplicación, hasta que sean derogadas o sustituidas por las normas o directrices que se adopten en virtud del artículo 13 de la Decisión (UE, Euratom) 2017/46.

Artículo 11

Entrada en vigor

La presente Decisión entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 6 de abril de 2018.

Por la Comisión,
en nombre del Presidente,
Günther OETTINGER
Miembro de la Comisión

ANEXO

FUNCIONES Y RESPONSABILIDADES (RASCI)

El modelo RASCI asigna funciones y responsabilidades a las entidades utilizando las siguientes abreviaturas:

a) R — ser responsable

b) A — rendir cuentas

c) S — prestar apoyo

d) C — ser consultado

e) I — estar informado

Función / Proceso	ISSB	HR (DS)	Servicios de la Comisión	Propietario del sistema	Propietario de los datos	LISO	DIGIT	Contratistas
Conformidad con la política de seguridad de la información de la Comisión		**R/A**	**S**				**S**	
Tecnologías de cifrado		**C**	**A**	**R**	**I**	**C**		
Inspecciones de seguridad informática	**I**	**A/R**		**S**	**I**	**I**	**S**	
Acceso desde redes externas	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externalización de SIC		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Todos los servicios de la Comisión excepto la Dirección General de Informática consultan al ISSB en relación con el funcionamiento de las redes internas.

[2] El propietario del sistema de un SIC que se externalice será responsable, y el propietario del sistema de cualquier otro SIC con el que un SIC externalizado esté interconectado será consultado.