DECISIONES

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

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,

Considerando lo siguiente:

(1) Los sistemas de información y comunicación de la Comisión forman parte integrante del funcionamiento de esta, y los incidentes de seguridad informática puede tener una incidencia decisiva sobre las operaciones de la Comisión y sobre determinados terceros, ya sean particulares, empresas o Estados miembros.

(2) Existen numerosas amenazas que pueden afectar a la confidencialidad, integridad o disponibilidad de los sistemas de información y comunicación de la Comisión, así como de la información que en ellos se procesa. Entre ellas figuran accidentes, errores, ataques deliberados y catástrofes naturales, que deben reconocerse como riesgos operativos.

(3) Los sistemas de información y comunicación deben contar con un nivel de protección acorde con la probabilidad, incidencia y naturaleza de los riesgos a que están expuestos.

(4) La seguridad informática en la Comisión debe garantizar que los SIC de la Comisión protegen la información que procesan y funcionan como y cuando deben funcionar, bajo el control de usuarios legítimos.

(5) La política de seguridad informática de la Comisión debe aplicarse de manera coherente con sus demás políticas de seguridad.

(6) La Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad tiene la responsabilidad general de la seguridad en la Comisión, bajo la autoridad y responsabilidad del miembro de la Comisión encargado de la seguridad.

(7) El enfoque de la Comisión debe tener en cuenta las iniciativas políticas y la legislación de la UE sobre seguridad de las redes y la información, las normas de la industria y las buenas prácticas, a fin de dar cumplimiento a toda la legislación pertinente y hacer posibles la interoperabilidad y la compatibilidad.

(8) Los servicios de la Comisión responsables de los sistemas de información y comunicación deben elaborar y aplicar las medidas oportunas, y deben coordinarse en toda la Comisión las medidas de seguridad informática para la protección de los sistemas de información y comunicación a fin de garantizar su eficiencia y eficacia.

(9) Las normas y procedimientos de acceso a la información en el contexto de la seguridad informática, incluida la gestión de los incidentes de seguridad informática, deben guardar proporción con la amenaza que representan para la Comisión o su personal y ajustarse a los principios establecidos en el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([1]), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Unión y a la libre circulación de estos datos, así como tener en cuenta el principio de secreto profesional, de conformidad con lo dispuesto en el artículo 339 del TFUE.

([1]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(10) Las políticas y normas relativas a los sistemas de información y comunicación que procesen información clasificada de la UE (ICUE), información sensible no clasificada e información no clasificada deben estar plenamente en consonancia con las Decisiones (UE, Euratom) 2015/443 ([1]) y (UE, Euratom) 2015/444 ([2]) de la Comisión.

(11) Es necesario que la Comisión revise y actualice las disposiciones sobre la seguridad de los sistemas de información y comunicación por ella utilizados.

(12) Por consiguiente, procede derogar la Decisión C(2006) 3602 de la Comisión.

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Decisión se aplicará a todos los sistemas de información y comunicación (SIC) poseídos, adquiridos, gestionados u operados por la Comisión o en su nombre y a todos los usos que haga la Comisión de estos SIC.

2. La presente Decisión establece los principios básicos, los objetivos, la organización y las responsabilidades en lo que respecta a la seguridad de estos SIC y, en particular, a los servicios de la Comisión que posean, adquieran, gestionen u operen SIC, incluidos los SIC facilitados por un prestador de servicios informáticos interno. Cuando un SIC sea aportado, poseído, gestionado u operado por un tercero externo sobre la base de un acuerdo bilateral o de un contrato con la Comisión, las condiciones del acuerdo o contrato deberán ajustarse a la presente Decisión.

3. La presente Decisión se aplicará a todos los servicios de la Comisión y agencias ejecutivas. Cuando un SIC de la Comisión sea utilizado por otros organismos o instituciones sobre la base de un acuerdo bilateral con la Comisión, las condiciones del acuerdo deberán ajustarse a la presente Decisión.

4. Sin perjuicio de eventuales indicaciones específicas relativas a grupos concretos de personal, la presente Decisión se aplicará a los miembros de la Comisión, al personal de la Comisión incluido en el ámbito de aplicación del Estatuto de los funcionarios de la Unión Europea («Estatuto de los funcionarios») y del régimen aplicable a los otros agentes de la Unión («ROA») ([3]), a los expertos nacionales en comisión de servicios en la Comisión («expertos nacionales») ([4]), a los proveedores de servicios externos y su personal, a los becarios y a cualquier persona con acceso a los SIC incluidos en el ámbito de la presente Decisión.

5. La presente Decisión se aplicará a la Oficina Europea de Lucha contra el Fraude (OLAF) en la medida en que ello sea compatible con la legislación de la Unión y la Decisión 1999/352/CE, CECA, Euratom de la Comisión ([5]). En particular, las medidas previstas en la presente Decisión, incluidas las instrucciones, inspecciones, investigaciones y medidas de efecto equivalente, podrán no aplicarse al SIC de la Oficina cuando ello no resulte compatible con la independencia de la función de investigación de la Oficina y/o la confidencialidad de la información obtenida por la Oficina en el ejercicio de dicha función.

Artículo 2

Definiciones

A efectos de la presente Decisión, se entenderá por:

1) «rendir cuentas», tener que responder acerca de las acciones, las decisiones y el rendimiento;

([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).

([2]) 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).

([3]) Establecido por el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (Estatuto de los funcionarios) (DO L 56 de 4.3.1968, p. 1).

([4]) Decisión de la Comisión de 12 de noviembre de 2008, relativa al régimen aplicable a los expertos nacionales en comisión de servicio y a los expertos nacionales en formación profesional destinados en los servicios de la Comisión [C(2008) 6866 final].

([5]) Decisión 1999/352/CE, CECA, Euratom de la Comisión, de 28 de abril de 1999, por la que se crea la Oficina Europea de Lucha contra el Fraude (DO L 136 de 31.5.1999, p. 20).

2) «CERT-EU»: el equipo de respuesta a emergencias informáticas de las instituciones y agencias de la UE. Su misión es ayudar a las instituciones europeas a protegerse de ataques maliciosos e intencionados que puedan poner en peligro la integridad de sus recursos informáticos y perjudicar a los intereses de la UE. El ámbito de las actividades de CERT-EU cubre la prevención, detección, respuesta y recuperación;

3) «servicio de la Comisión»: toda Dirección General o departamento de la Comisión, o cualquier gabinete de un miembro de la Comisión;

4) «autoridad de seguridad de la Comisión»: la función establecida en la Decisión (UE, Euratom) 2015/444;

5) «sistema de información y comunicación» o «SIC»: todo sistema que permita el tratamiento de información en formato electrónico, incluyendo todos los activos necesarios para su funcionamiento, así como la infraestructura, organización, personal y recursos de información. Esta definición incluye las aplicaciones profesionales, los servicios informáticos compartidos, los sistemas externalizados y los dispositivos de los usuarios finales;

6) «Consejo de Administración»: aporta el máximo nivel de supervisión de la gestión de las cuestiones administrativas y operativas en la Comisión;

7) «propietario de datos»: la persona responsable de garantizar la protección y utilización de un conjunto de datos específico gestionado por un SIC;

8) «conjunto de datos»: un conjunto de información que sirve a un proceso o actividad específicos de la Comisión;

9) «procedimiento de emergencia»: un conjunto predefinido de métodos y responsabilidades para hacer frente a situaciones de urgencia con el fin de evitar una incidencia importante sobre la Comisión;

10) «política de seguridad de la información»: una serie de objetivos en materia de seguridad de la información que se han establecido, aplicado y comprobado o deben serlo. Incluye, sin limitarse a ellas, las Decisiones (UE, Euratom) 2015/444 y (UE, Euratom) 2015/443;

11) «Consejo Director de Seguridad de la Información (ISSB)»: el órgano de gobierno que apoya al Consejo de Administración en sus tareas relacionadas con la seguridad informática;

12) «proveedor de servicios informáticos interno»: un servicio de la Comisión que presta servicios informáticos compartidos;

13) «seguridad informática» o «seguridad de los SIC»: la preservación de la confidencialidad, integridad y disponibilidad de los SIC y los conjuntos de datos que procesan;

14) «directrices de seguridad informática»: las medidas recomendadas, pero voluntarias, que contribuyen a sustentar las normas de seguridad informática o sirven de referencia cuando no existen normas aplicables;

15) «incidente de seguridad informática»: un suceso que podría afectar negativamente a la confidencialidad, integridad o disponibilidad de un SIC;

16) «medida de seguridad informática»: una medida técnica u organizativa destinada a atenuar los riesgos de seguridad informática;

17) «necesidad de seguridad informática»: una definición precisa e inequívoca de los niveles de confidencialidad, integridad y disponibilidad asociados a una información o a un sistema informático con vistas a determinar el nivel de protección requerido;

18) «objetivo de seguridad informática»: una declaración de intenciones para luchar contra amenazas concretas y/o satisfacer determinados requisitos o supuestos de seguridad organizativa especificados;

19) «plan de seguridad informática»: la documentación de las medidas de seguridad informática necesarias para satisfacer las necesidades de seguridad informática de un SIC;

20) «política de seguridad informática»: una serie de objetivos en materia de seguridad informática que se han establecido, aplicado y comprobado o deben serlo. Incluye la presente Decisión y sus disposiciones de aplicación;

21) «requisito de seguridad informática»: una necesidad de seguridad informática formalizada a través de un proceso predefinido;

22) «riesgo para la seguridad informática»: un efecto que una amenaza para la seguridad informática podría inducir en un SIC explotando una vulnerabilidad. En este sentido, un riesgo para la seguridad informática se caracteriza por dos factores: 1) incertidumbre, es decir, la probabilidad de que una amenaza a la seguridad informática cause un acontecimiento no deseado, y 2) incidencia, es decir, las consecuencias que puede tener dicho acontecimiento no deseado para un SIC;

23) «normas de seguridad informática»: las medidas de seguridad informática obligatorias específicas que contribuyen a aplicar y sostener la política de seguridad informática;

24) «estrategia de seguridad informática»: un conjunto de proyectos y actividades destinados al logro de los objetivos de la Comisión y que deben establecerse, aplicarse y controlarse;

25) «amenaza para la seguridad informática»: un factor que puede potencialmente conducir a un acontecimiento no deseado que ocasione daños a un SIC. Estas amenazas pueden ser accidentales o deliberadas y se caracterizan por los elementos amenazadores, las posibles dianas y los métodos de ataque;

26) «responsable local de seguridad informática» o «LISO»: el funcionario que actúa de enlace para la seguridad informática en un servicio de la Comisión;

27) «datos personales», «tratamiento de datos personales», «responsable del tratamiento» y «fichero de datos personales»: tienen el mismo significado que en el Reglamento (CE) n.º 45/2001, y en particular su artículo 2;

28) «tratamiento de la información»: todas las funciones de un SIC con respecto a los conjuntos de datos, incluidos la creación, modificación, presentación, almacenamiento, transporte, supresión y archivado de la información. El tratamiento de la información puede efectuarlo un SIC como conjunto de funcionalidades destinadas a los usuarios y como servicios informáticos prestados a otros SIC;

29) «secreto profesional»: la protección de los datos comerciales de la categoría amparada por la obligación de secreto profesional, en particular la información sobre las empresas, sus relaciones comerciales o los elementos de sus costes según establece el artículo 339 del TFUE;

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

31) «seguridad en la Comisión»: la seguridad de las personas, los bienes y la información de la Comisión, y en particular la integridad física de las personas y los bienes, la integridad, confidencialidad y disponibilidad de la información y de los sistemas de información y comunicación, así como el funcionamiento sin trabas de las operaciones de la Comisión;

32) «servicio informático compartido»: el servicio que ofrece un SIC a otros SIC para el tratamiento de la información;

33) «propietario del sistema»: la persona responsable globalmente de la adquisición, el desarrollo, la integración, la modificación, la explotación, el mantenimiento y la retirada de un SIC;

34) «usuario»: toda persona que utilice la funcionalidad proporcionada por un SIC, ya sea dentro o fuera de la Comisión.

Artículo 3

Principios de seguridad informática en la Comisión

1. La seguridad informática en la Comisión se basará en los principios de legalidad, transparencia, proporcionalidad y rendición de cuentas.

2. Los aspectos de seguridad informática se tendrán en cuenta desde el inicio del desarrollo y la implantación de los SIC de la Comisión. A tal efecto, la Dirección General de Informática y la Dirección General de Recursos Humanos y Seguridad intervendrán en sus respectivos ámbitos de responsabilidad.

3. Una seguridad informática eficaz garantizará unos niveles apropiados de:

a) autenticidad: garantía de que la información es verídica y procede de fuentes de buena fe;

b) disponibilidad: propiedad de ser accesible y utilizable en el momento en que lo requiera una entidad autorizada;

c) confidencialidad: propiedad de que la información no se revele a personas, organismos o procesos no autorizados;

d) integridad: propiedad de salvaguardar la exactitud y completitud de la información y los activos;

e) no repudio: capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente;

f) protección de datos personales: provisión de salvaguardias adecuadas en relación con los datos personales, respetando plenamente el Reglamento (CE) n.º 45/2001;

g) secreto profesional: la protección de la información de la categoría amparada por la obligación de secreto profesional, en particular la información sobre las empresas, sus relaciones comerciales o los elementos de sus costes según establece el artículo 339 del TFUE.

4. La seguridad informática se basará en un proceso de gestión del riesgo. Este proceso tendrá por objeto determinar los niveles de los riesgos de seguridad informática y definir medidas de seguridad para reducirlos a un nivel adecuado con un coste proporcionado.

5. Todos los SIC deberán ser identificados, adscritos a un propietario del sistema y registrados en un inventario.

6. Los requisitos de seguridad de todos los SIC se determinarán sobre la base de sus necesidades de seguridad y de las necesidades de seguridad de la información que procesen. Los SIC que presten servicios a otros SIC podrán estar diseñados para soportar determinados niveles de necesidades de seguridad.

7. Los planes de seguridad informática y las medidas de seguridad informática guardarán proporción con las necesidades de seguridad del SIC.

Los procesos relacionados con estos principios y actividades deberán pormenorizarse mediante disposiciones de aplicación.

CAPÍTULO 2

ORGANIZACIÓN Y RESPONSABILIDADES

Artículo 4

Consejo de Administración

El Consejo de Administración tendrá la responsabilidad general de la gobernanza de la seguridad informática en su conjunto dentro de la Comisión.

Artículo 5

Consejo Director de Seguridad de la Información (ISSB)

1. El ISSB estará presidido por el secretario general adjunto responsable de la gobernanza de la seguridad informática en la Comisión. Sus miembros representarán los intereses de la seguridad, la tecnología y la actividad de los distintos servicios de la Comisión e incluirán a representantes de la Dirección General de Informática, la Dirección General de Recursos Humanos y Seguridad, la Dirección General de Presupuesto y, en rotación bienal, de otros cuatro servicios de la Comisión involucrados para cuyo funcionamiento constituya una preocupación importante la seguridad informática. Los miembros deberán ocupar cargos superiores de dirección.

2. El ISSB prestará apoyo al Consejo de Administración en sus tareas relacionadas con la seguridad informática. Tendrá asimismo la responsabilidad operativa de la gobernanza de la seguridad informática en su conjunto dentro de la Comisión.

3. El ISSB recomendará la política de seguridad informática de la Comisión para su adopción por esta.

4. Asimismo, revisará e informará semestralmente al Consejo de Administración sobre cuestiones de gobernanza, así como sobre cuestiones relacionadas con la seguridad, incluidos los incidentes graves de seguridad informática.

5. El ISSB supervisará y evaluará la ejecución general de la presente Decisión e informará al respecto al Consejo de Administración.

6. A propuesta de la Dirección General de Informática, el ISSB examinará, aprobará y supervisará la aplicación de la estrategia móvil de seguridad informática. Informará al respecto al Consejo de Administración.

7. El ISSB supervisará, evaluará y controlará la situación de los riesgos para la información corporativa y estará facultado para expedir peticiones oficiales de mejoras siempre que sea necesario.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 6

Dirección General de Recursos Humanos y Seguridad

Por lo que se refiere a la seguridad informática, la Dirección General de Recursos Humanos y Seguridad asumirá las responsabilidades siguientes. Deberá:

1) garantizar la armonización entre la política de seguridad informática y la política de seguridad de la información de la Comisión;

2) crear un marco para la autorización del uso de tecnologías de cifrado para el almacenamiento y la comunicación de información por parte de los SIC;

3) informar a la Dirección General de Informática sobre amenazas específicas que puedan tener incidencia significativa en la seguridad de los SIC y los conjuntos de datos que procesan;

4) realizar inspecciones de seguridad informática para evaluar la conformidad de los SIC de la Comisión con la política de seguridad y comunicar los resultados al ISSB;

5) crear un marco para la autorización del acceso, y las correspondientes reglas de seguridad apropiadas, a los SIC de la Comisión desde redes externas y elaborar las directrices y normas de seguridad informática conexas, en estrecha cooperación con la Dirección General de Informática;

6) proponer principios y reglas para la externalización de los SIC con objeto de mantener un control adecuado de la seguridad de la información;

7) elaborar las correspondientes directrices y normas de seguridad informática en relación con el artículo 6, en estrecha cooperación con la Dirección General de Informática.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 7

Dirección General de Informática

Por lo que se refiere a la seguridad informática global de la Comisión, la Dirección General de Informática tendrá las siguientes responsabilidades. Deberá:

1) elaborar normas y directrices de seguridad informática, con excepción de lo dispuesto en el artículo 6, en estrecha cooperación con la Dirección General de Recursos Humanos y Seguridad, con vistas a asegurar la coherencia entre la política de seguridad informática y la política de seguridad de la información de la Comisión, y proponerlas al ISSB;

2) evaluar los métodos, procesos y resultados de gestión de los riesgos para la seguridad informática de todos los servicios de la Comisión e informar periódicamente al respecto al ISSB;

3) proponer una estrategia móvil de seguridad informática para su revisión y aprobación por el ISSB y ulterior adopción por el Consejo de Administración, y proponer un programa, incluida la planificación de los proyectos y actividades por los que se aplique la estrategia de seguridad informática;

4) supervisar la ejecución de la estrategia de seguridad informática de la Comisión e informar al respecto periódicamente al ISSB;

5) supervisar los riesgos para la seguridad informática y las medidas de seguridad informática aplicadas en los SIC e informar al respecto periódicamente al ISSB;

6) informar periódicamente al ISSB sobre la ejecución general y el cumplimiento de la presente Decisión;

7) previa consulta con la Dirección General de Recursos Humanos y Seguridad, solicitar a los propietarios de sistemas que tomen determinadas medidas de seguridad informática a fin de atenuar los riesgos para la seguridad informática de los SIC de la Comisión;

8) garantizar que exista un catálogo adecuado de servicios de seguridad informática de la Dirección General de Informática a disposición de los propietarios de sistemas y los propietarios de datos para facilitarles el desempeño de sus responsabilidades en materia de seguridad informática y el cumplimiento de las normas y la política de seguridad informática;

9) ofrecer una documentación adecuada a los propietarios de sistemas y de datos y evacuar consultas con ellos, cuando proceda, sobre las medidas de seguridad informática aplicadas en sus servicios informáticos a fin de facilitar el cumplimiento de la política de seguridad informática y prestar apoyo a los propietarios de sistemas en la gestión de los riesgos informáticos;

10) organizar periódicamente reuniones de la red de LISO y prestar apoyo a estos en el desempeño de sus funciones;

11) definir las necesidades de formación y coordinar los programas de formación sobre seguridad informática en cooperación con los servicios de la Comisión, y desarrollar, ejecutar y coordinar campañas de sensibilización sobre la seguridad informática en estrecha cooperación con la Dirección General de Recursos Humanos;

12) garantizar que los propietarios de sistemas, los propietarios de datos y otras funciones con responsabilidades de seguridad informática en los servicios de la Comisión estén al tanto de la política de seguridad informática;

13) informar a la Dirección General de Recursos Humanos y Seguridad sobre las amenazas específicas para la seguridad informática, los incidentes y las excepciones a la política de seguridad informática de la Comisión notificadas por los propietarios de sistemas que puedan tener una incidencia importante sobre la seguridad en la Comisión;

14) por lo que se refiere a su papel de proveedor de servicios informáticos internos, presentar a la Comisión un catálogo de servicios informáticos compartidos que prevean niveles definidos de seguridad; tal cosa se realizará evaluando, gestionando y supervisando sistemáticamente los riesgos para la seguridad informática, a fin de aplicar las medidas de seguridad que permitan alcanzar el nivel de seguridad definido.

Los procesos conexos y responsabilidades más detalladas se definirán pormenorizadamente mediante disposiciones de aplicación.

Artículo 8

Servicios de la Comisión

Por lo que se refiere a la seguridad informática en su servicio, cada jefe de servicio de la Comisión deberá:

1) designar oficialmente para cada SIC un propietario del sistema, funcionario o agente temporal, que será el responsable de la seguridad informática de ese SIC y designar oficialmente un propietario de los datos para cada conjunto de datos gestionados en un SIC, que debe pertenecer a la misma entidad administrativa que sea el responsable del tratamiento de datos para los conjuntos de datos sujetos al Reglamento (CE) n.º 45/2001;

2) designar oficialmente un responsable local de seguridad informática (LISO) que pueda desempeñar las responsabilidades con independencia de los propietarios de sistemas y los propietarios de datos; se podrá designar un LISO para uno o varios servicios de la Comisión;

3) velar por que se hayan realizado y aplicado las evaluaciones de riesgos para la seguridad informática y los planes de seguridad informática apropiados;

4) velar por que se comunique periódicamente un resumen de los riesgos y medidas de seguridad informática a la Dirección General de Informática;

5) velar, con el apoyo de la Dirección General de Informática, por la implantación de los procesos, procedimientos y soluciones adecuados para garantizar la detección, notificación y resolución eficientes de los incidentes de seguridad informática relativos a sus SIC;

6) poner en marcha un procedimiento de emergencia en caso de emergencias de seguridad informática;

7) rendir cuentas en última instancia sobre la seguridad informática, incluidas las responsabilidades de los propietarios de sistemas y los propietarios de datos;

8) asumir los riesgos ligados a sus propios SIC y conjuntos de datos;

9) resolver los eventuales desacuerdos entre los propietarios de datos y los propietarios de sistemas y, en caso de persistir el desacuerdo, someter el asunto al ISSB para su resolución;

10) velar por que se apliquen los planes y las medidas de seguridad informática y por que los riesgos estén adecuadamente cubiertos.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 9

Propietarios de sistemas

1. El propietario del sistema es responsable de la seguridad informática del SIC bajo la autoridad del jefe del servicio de la Comisión.

2. Por lo que se refiere a la seguridad informática, el propietario del sistema deberá:

a) velar por la conformidad del SIC con la política de seguridad informática;

b) velar por que el SIC esté adecuadamente registrado en el inventario correspondiente;

c) evaluar los riesgos para la seguridad informática y determinar las necesidades de seguridad informática de cada SIC, en colaboración con los propietarios de datos y en consulta con la Dirección General de Informática;

d) preparar un plan de seguridad que incluya, cuando proceda, detalles relativos a los riesgos evaluados y las medidas de seguridad adicionales necesarias;

e) aplicar las medidas de seguridad informática apropiadas, proporcionales a los riesgos para la seguridad informática identificados y siguiendo las recomendaciones aprobadas por el ISSB;

f) detectar cualquier dependencia respecto de otros SIC o servicios informáticos compartidos y aplicar las medidas de seguridad adecuadas en función de los niveles de seguridad propuestos por dichos SIC o servicios informáticos compartidos;

g) gestionar y supervisar los riesgos para la seguridad informática;

h) informar periódicamente al jefe del servicio de la Comisión sobre el perfil de riesgo para la seguridad informática de su SIC e informar a la Dirección General de Informática sobre los riesgos conexos, las actividades de gestión del riesgo y las medidas de seguridad adoptadas;

i) consultar al LISO del servicio o los servicios de la Comisión pertinentes sobre aspectos de la seguridad informática;

j) publicar instrucciones destinadas a los usuarios sobre la utilización del SIC y los datos asociados, así como sobre las responsabilidades de los usuarios en relación con el SIC;

k) solicitar autorización de la Dirección General de Recursos Humanos y Seguridad, en calidad de autoridad criptográfica, para cualquier SIC que utilice tecnología de cifrado;

l) consultar por adelantado a la autoridad de seguridad de la Comisión con respecto a los sistemas que procesen información clasificada de la UE;

m) velar por que las copias de seguridad de las claves de descifrado se almacenen en una cuenta bloqueada; la recuperación de datos cifrados se llevará a cabo solo cuando esté autorizada de conformidad con el marco definido por la Dirección General de Recursos Humanos y Seguridad;

n) respetar todas las instrucciones del responsable o los responsables del tratamiento pertinentes referidas a la protección de los datos personales y la aplicación de las reglas sobre protección de datos a la seguridad del tratamiento;

o) notificar a la Dirección General de Informática las posibles excepciones a la política de seguridad informática de la Comisión, incluyendo las justificaciones pertinentes;

p) informar al jefe del servicio de la Comisión de cualquier desacuerdo insuperable entre el propietario de datos y el propietario del sistema, y comunicar oportunamente los incidentes de seguridad informática a las partes interesadas, según proceda en función de su gravedad, con arreglo a lo dispuesto en el artículo 15;

q) en el caso de los sistemas externalizados, velar por que se incluyan las disposiciones sobre seguridad informática adecuadas en los contratos de externalización y por que los incidentes de seguridad que se produzcan en los SIC externalizados se notifiquen de conformidad con el artículo 15;

r) en el caso de los SIC que prestan servicios informáticos compartidos, garantizar que se ofrece un nivel de seguridad definido, claramente documentado y que se aplican medidas de seguridad en ese SIC a fin de alcanzar el nivel de seguridad definido.

3. Los propietarios de sistemas podrán delegar oficialmente una parte o la totalidad de sus tareas de seguridad informática, pero seguirán siendo responsables de la seguridad informática de sus SIC.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 10

Propietarios de datos

1. El propietario de datos es responsable de la seguridad informática de un conjunto de datos específico ante el jefe del servicio de la Comisión y debe rendir cuentas de la confidencialidad, integridad y disponibilidad de dicho conjunto.

2. Por lo que se refiere a este conjunto de datos, el propietario de datos deberá:

a) velar por que todos los conjuntos de datos bajo su responsabilidad se clasifiquen adecuadamente de conformidad con las Decisiones (UE, Euratom) 2015/443 y (UE, Euratom) 2015/444;

b) definir las necesidades de seguridad de la información e informar a los propietarios de sistemas pertinentes acerca de estas necesidades;

c) participar en la evaluación del riesgo del SIC;

d) comunicar al jefe del servicio de la Comisión cualquier desacuerdo insuperable entre el propietario de datos y el propietario del sistema;

e) comunicar los incidentes de seguridad informática conforme a lo dispuesto en el artículo 15.

3. Los propietarios de datos podrán delegar oficialmente una parte o la totalidad de sus tareas de seguridad informática, pero mantendrán sus responsabilidades según se definen en el presente artículo.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 11

Responsables locales de seguridad informática (LISO)

Por lo que se refiere a la seguridad informática, el LISO deberá:

a) identificar de manera proactiva a los propietarios de sistemas, los propietarios de datos y otras funciones con responsabilidades de seguridad informática en los servicios de la Comisión e informarles acerca de la política de seguridad informática;

b) servir de enlace sobre cuestiones relacionadas con la seguridad informática en los servicios de la Comisión con la Dirección General de Informática, en el marco de la red de LISO;

c) asistir a las reuniones periódicas de LISO;

d) mantener una visión general del proceso de gestión de riesgos para la seguridad de la información y del desarrollo y aplicación de los planes de seguridad del sistema de información;

e) asesorar a los propietarios de datos, a los propietarios de sistemas y a los jefes de los servicios de la Comisión sobre temas relacionados con la seguridad informática;

f) cooperar con la Dirección General de Informática en la difusión de buenas prácticas de seguridad informática y proponer programas específicos de sensibilización y programas de formación;

g) presentar al jefe del servicio o los servicios de la Comisión informes sobre la seguridad informática, las carencias detectadas y las posibles mejoras.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse mediante disposiciones de aplicación.

Artículo 12

Usuarios

1. Por lo que se refiere a la seguridad informática, los usuarios deberán:

a) respetar la política de seguridad informática y las instrucciones impartidas por el propietario del sistema para el uso de cada SIC;

b) comunicar los incidentes de seguridad informática conforme a lo dispuesto en el artículo 15.

2. La utilización de los SIC de la Comisión en contravención de la política de seguridad informática o de las instrucciones impartidas por el propietario del sistema podría dar lugar a procedimientos disciplinarios.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse en disposiciones de aplicación.

CAPÍTULO 3

REQUISITOS Y OBLIGACIONES EN MATERIA DE SEGURIDAD

Artículo 13

Aplicación de la Decisión

1. La adopción de las disposiciones de aplicación relativas al artículo 6, así como de las correspondientes normas y directrices, será objeto de una decisión de habilitación de la Comisión en favor del miembro de la Comisión responsable de los asuntos de seguridad.

2. La adopción de todas las demás disposiciones de aplicación relativas a la presente Decisión, así como de las correspondientes normas y directrices de seguridad informática, será objeto de una decisión de habilitación de la Comisión en favor del miembro de la Comisión responsable de la informática.

3. El ISSB aprobará las disposiciones de aplicación, normas y directrices mencionadas en los apartados 1 y 2 antes de su adopción.

Artículo 14

Obligación de cumplimiento

1. El cumplimiento de las disposiciones recogidas en la política y las normas de seguridad informática es obligatorio.

2. El incumplimiento de la política y las normas de seguridad informática podrá dar lugar a medidas disciplinarias de conformidad con los Tratados, el Estatuto de los funcionarios y el régimen aplicable a los otros agentes de la Unión, a sanciones contractuales y/o a acciones judiciales de conformidad con las disposiciones legales y reglamentarias nacionales.

3. La Dirección General de Informática será notificada acerca de cualquier excepción a la política de seguridad informática.

4. En el caso de que el ISSB entienda que existe un riesgo inaceptable y persistente para un SIC de la Comisión, la Dirección General de Informática, en cooperación con el propietario del sistema, someterá a la aprobación del ISSB unas medidas paliativas. Dichas medidas podrán incluir, entre otras cosas, el refuerzo de la supervisión y la presentación de informes, la restricción de los servicios y la desconexión.

5. El ISSB deberá imponer la aplicación de las medidas paliativas aprobadas cuando sea necesario. El ISSB también podrá recomendar al Director General de la Dirección General de Recursos Humanos y Seguridad la apertura de una investigación administrativa. La Dirección General de Informática informará al ISSB sobre todos los casos en que se impongan medidas paliativas.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse en disposiciones de aplicación.

Artículo 15

Tratamiento de los incidentes de seguridad informática

1. La Dirección General de Informática será responsable de aportar la principal capacidad de respuesta operativa ante incidentes de seguridad informática dentro de la Comisión Europea.

2. La Dirección General de Recursos Humanos y Seguridad, como parte interesada en la respuesta ante incidentes de seguridad informática:

a) tendrá derecho a acceder a la información resumida de todos los registros de incidentes, y a los registros completos previa solicitud;

b) participará en los grupos de gestión de crisis para los incidentes de seguridad informática y en los procedimientos de emergencia de seguridad informática;

c) se encargará de las relaciones con las fuerzas y cuerpos de seguridad y los servicios de inteligencia;

d) llevará a cabo análisis forenses sobre ciberseguridad de conformidad con el artículo 11 de la Decisión (UE, Euratom) 2015/443;

e) tomará una decisión sobre la necesidad de iniciar una investigación oficial;

f) informará a la Dirección General de Informática de cualquier incidente relacionado con la seguridad informática que pueda crear un riesgo para otros SIC.

3. Se celebrarán contactos periódicos entre la Dirección General de Informática y la Dirección General de Recursos Humanos y Seguridad para intercambiar información y coordinar la gestión de los incidentes de seguridad, y en particular de los incidentes de seguridad informática que puedan exigir una investigación oficial.

4. Los servicios de coordinación de incidentes del equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos europeos (CERT-EU) podrán prestar su apoyo al proceso de gestión de incidentes cuando proceda y compartir conocimientos con otras instituciones y organismos de la UE que puedan verse afectados.

5. Los propietarios de sistemas implicados en un incidente de seguridad informática deberán:

a) notificar inmediatamente a su jefe de servicio de la Comisión, a la Dirección General de Informática, a la Dirección General de Recursos Humanos, al LISO y, en su caso, al propietario de los datos todos los incidentes de seguridad informática importantes, en particular los que impliquen una violación de la confidencialidad de los datos;

b) cooperar y seguir las instrucciones de las autoridades pertinentes de la Comisión relativas a la comunicación, respuesta y rehabilitación en caso de incidente.

6. Los usuarios comunicarán oportunamente todos los incidentes de seguridad informática reales o presuntos al servicio de asistencia informática que corresponda.

7. Los propietarios de datos comunicarán oportunamente todos los incidentes de seguridad informática reales o presuntos al equipo de respuesta a incidentes de seguridad informática que corresponda.

8. La Dirección General de Informática, con el respaldo de las demás partes interesadas, será responsable de la gestión de cualquier incidente de seguridad informática detectado en relación con los SIC de la Comisión que no hayan sido externalizados.

9. La Dirección General de Informática informará acerca de los incidentes de seguridad informática a los servicios de la Comisión afectados, a los LISO pertinentes y, si procede, al CERT-EU en la medida en que deban conocerlos.

10. La Dirección General de Informática presentará informes periódicos al ISSB sobre los incidentes de seguridad informática importantes que afecten a los SIC de la Comisión.

11. El LISO pertinente, previa petición, podrá acceder a los registros de incidentes de seguridad informática relativos al SIC del servicio de la Comisión.

12. En caso de incidente de seguridad informática importante, la Dirección General de Informática será el punto de contacto para la gestión de las situaciones de crisis, encargándose de coordinar a los grupos de gestión de crisis de los incidentes de seguridad informática.

13. En caso de emergencia, el Director General de la Dirección General de Informática podrá tomar la decisión de poner en marcha un procedimiento de emergencia de seguridad informática. La Dirección General de Informática elaborará procedimientos de emergencia que deberá aprobar el ISSB.

14. La Dirección General de Informática informará sobre la ejecución de los procedimientos de emergencia al ISSB y a los jefes de los servicios de la Comisión afectados.

Los procesos relacionados con estas responsabilidades y actividades deberán pormenorizarse en disposiciones de aplicación.

CAPÍTULO 4

DISPOSICIONES FINALES

Artículo 16

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 17

Relación con otros actos

Lo dispuesto en la presente Decisión se entenderá sin perjuicio de la Decisión (UE, Euratom) 2015/443, la Decisión (UE, Euratom) 2015/444, el Reglamento (CE) n.º 45/2001, el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo ([1]), la Decisión 2002/47/CE, CECA, Euratom de la Comisión ([2]), el Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo ([3]) y la Decisión 1999/352/CE, CECA, Euratom.

Artículo 18

Derogación y medidas transitorias

Queda derogada la Decisión C(2006) 3602 de 16 de agosto de 2006.

Las disposiciones de aplicación y las normas de seguridad informática adoptadas en virtud del artículo 10 de la Decisión C(2006) 3602 permanecerán en vigor, siempre que no entren en conflicto con la presente Decisión, hasta que sean sustituidas por las disposiciones de aplicación y las normas que se adopten en virtud del artículo 13 de la presente Decisión. Toda referencia al artículo 10 de la Decisión C(2006) 3602 se entenderá hecha al artículo 13 de la presente Decisión.

Artículo 19

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 10 de enero de 2017.

Por la Comisión
El Presidente
Jean-Claude JUNCKER

([1]) Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

([2]) Decisión 2002/47/CE, CECA, Euratom de la Comisión, de 23 de enero de 2002, por la que se modifica su Reglamento interno (DO L 21 de 24.1.2002, p. 23).

([3]) Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) y por el que se deroga el Reglamento (CE) n.º 1073/1999 del Parlamento Europeo y del Consejo y el Reglamento (Euratom) n.º 1074/1999 del Consejo (DO L 248 de 18.9.2013, p. 1).