DECISIÓN (UE) 2022/640 DE LA COMISIÓN

de 7 de abril de 2022

sobre las normas de desarrollo relativas a las funciones y responsabilidades de los principales agentes en el ámbito de la seguridad

LA COMISIÓN EUROPEA,

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

Vista la Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión ([1]),

Vista la 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 ([2]),

Considerando lo siguiente:

(1) Las Decisiones (UE, Euratom) 2015/443 y (UE, Euratom) 2015/444 se aplican a todos los servicios y en todos los locales de la Comisión.

(2) En caso necesario, deben adoptarse normas de desarrollo para completar o facilitar la aplicación de la Decisión (UE, Euratom) 2015/444, de conformidad con el artículo 60 de esta.

(3) Las medidas de seguridad destinadas a proteger la información clasificada de la UE a lo largo de su ciclo de vida deben ser proporcionales, ante todo, a su clasificación de seguridad.

(4) Las medidas de seguridad destinadas a proteger los sistemas de información y comunicación de la Comisión se establecen en la Decisión (UE, Euratom) 2017/46 de la Comisión ([3]), en particular en su artículo 3, relativo a los principios de seguridad informática en la Comisión y en su artículo 9, relativo a los propietarios de sistemas.

(5) El objetivo de las normas de desarrollo relativas a las funciones y responsabilidades de los principales agentes en el ámbito de la seguridad es proporcionar orientaciones sobre los requisitos previos y obligaciones establecidos respecto de esas funciones en las Decisiones (UE, Euratom) 2015/443 y (UE, Euratom) 2015/444.

(6) El artículo 36, apartado 7, de la Decisión (UE, Euratom) 2015/444 establece una serie de funciones adicionales relacionadas con la seguridad que deben ser asumidas por la Autoridad de Seguridad de la Comisión. Las tareas correspondientes a dichas funciones se establecen mediante la presente Decisión.

(7) Los responsables locales de seguridad y los controladores del registro asumen responsabilidades específicas en materia de protección de la información clasificada de la UE en sus respectivos servicios, de conformidad con la Decisión (UE, Euratom) 2015/444.

(8) El 4 de mayo de 2016, la Comisión adoptó una Decisión ([4]) que facultaba al miembro de la Comisión responsable de los asuntos de seguridad para adoptar, en nombre de la Comisión y bajo su responsabilidad, las normas de desarrollo contempladas en el artículo 60 de la Decisión (UE, Euratom) 2015/444; posteriormente, el 13 de abril de 2021, el miembro de la Comisión responsable de los asuntos de seguridad adoptó, en nombre de la Comisión y bajo su responsabilidad, una Decisión ([5]) por la que se subdelegaban estas normas de desarrollo en el Director General de la Dirección General de Recursos Humanos y Seguridad.

([1]) DO L 72 de 17.3.2015, p. 41.
([2]) DO L 72 de 17.3.2015, p. 53.
([3]) 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 (DO L 6 de 11.1.2017, p. 40).
([4]) Decisión C(2016) 2797 de la Comisión, de 4 de mayo de 2016, relativa a una habilitación en materia de seguridad.
([5]) Decisión C(2021) 2684 de la Comisión, de 13 de abril de 2021, por la que se concede una subdelegación de poderes en virtud de la Decisión C(2016) 2797 de la Comisión, relativa a una habilitación en materia de seguridad.

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO 1

Disposiciones generales

Artículo 1

Objetivo y ámbito de aplicación

1. La presente Decisión establece las funciones y responsabilidades de los principales agentes en el ámbito de la seguridad encargados de la protección de la información clasificada de la UE (ICUE) en la Comisión en virtud de las Decisiones (UE, Euratom) 2015/443 y (UE, Euratom) 2015/444.

2. La presente Decisión se aplicará a todos los servicios de la Comisión y en todos los locales de la Comisión.

CAPÍTULO 2

Dirección General de Recursos Humanos y Seguridad

Artículo 2

Autoridad de Seguridad de la Comisión

1. El director de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad asumirá la función de Autoridad de Seguridad de la Comisión (CSA) a que se refiere el artículo 7 de la Decisión (UE, Euratom) 2015/444.

2. La CSA desempeñará sus funciones en los siguientes ámbitos, tal como se establece en la Decisión (UE, Euratom) 2015/444, de conformidad con los artículos 3 a 7 de la presente Decisión:

a) seguridad del personal;

b) seguridad física;

c) gestión de la ICUE;

d) acreditación de todo sistema de información y comunicaciones (SIC) que maneje ICUE;

e) seguridad industrial; e

f) intercambio de información clasificada.

3. La CSA dispensará formación obligatoria a los responsables locales de seguridad (LSO), a los LSO adjuntos, a los controladores del registro (RCO) y a los RCO adjuntos sobre sus responsabilidades y obligaciones.

Artículo 3

Autoridad de Garantía de la Información

La Autoridad de Garantía de la Información asumirá la responsabilidad de las siguientes actividades en relación con la protección de la ICUE:

a) desarrollar políticas de garantía de seguridad de la información y directrices de seguridad y supervisar su eficacia y su pertinencia;

b) salvaguardar y administrar la información técnica relacionada con los productos criptológicos;

c) garantizar que las medidas de garantía de la información se ajusten a las políticas de seguridad y contratación pública de la Comisión, según proceda;

d) garantizar que los productos criptológicos se seleccionen de conformidad con las normas que rigen su idoneidad y selección;

e) consultar a los propietarios, los proveedores de sistemas, los agentes en el ámbito de la seguridad y los representantes de los usuarios sobre las políticas de garantía de la seguridad de la información y las directrices de seguridad.

Artículo 4

Autoridad de Acreditación de Seguridad

1. La CSA será la responsable de la acreditación de las zonas de acceso restringido que cumplan los requisitos del artículo 18 de la Decisión 2015/444 y de los SIC para el manejo de ICUE.

2. Los servicios de la Comisión consultarán a la Autoridad de Acreditación de Seguridad, en coordinación con sus LSO y sus responsables locales de seguridad informática (LISO), según proceda, siempre que un servicio tenga la intención de:

a) construir una zona de acceso restringido;

b) implantar un SIC para manejar ICUE;

c) instalar cualquier otro equipo para el manejo de información clasificada, incluidas las conexiones a SIC de terceros.

La Autoridad de Acreditación de Seguridad ofrecerá asesoramiento sobre estas actividades tanto durante el proceso de planificación como durante el de construcción o desarrollo.

3. No se manejará ICUE en una zona de acceso restringido o en un SIC sin la previa expedición, por parte de la Autoridad de Acreditación de Seguridad, de una acreditación al nivel adecuado de ICUE.

4. Los requisitos de acreditación de una zona de acceso restringido incluirán:

a) la aprobación de los planes para la zona de acceso restringido;

b) la aprobación de todos los contratos de obras que realicen contratistas externos, teniendo en cuenta las disposiciones en materia de seguridad industrial, como, por ejemplo, los requisitos de habilitación de seguridad de los contratistas y de su personal;

c) la disponibilidad de todas las declaraciones y certificados de conformidad requeridos;

d) una inspección física de la zona de acceso restringido para comprobar que los materiales y métodos de construcción, los controles de acceso, los equipos de seguridad y cualquier otro elemento cumplen los requisitos establecidos por la CSA;

e) la validación de las medidas para contrarrestar las radiaciones electromagnéticas en cualquier zona de acceso restringido protegida por medios técnicos;

f) la aprobación de los procedimientos operativos de seguridad para la zona de acceso restringido.

5. Los requisitos de acreditación de un SIC que maneje ICUE incluirán:

a) la adopción de una estrategia de acreditación del sistema;

b) la validación del plan de seguridad del SIC, sobre la base de un enfoque de gestión de riesgos;

c) la validación de los procedimientos operativos de seguridad para el SIC;

d) la validación de todos los demás documentos de seguridad requeridos, según determine la Autoridad de Acreditación de Seguridad;

e) la aprobación del uso de cualquier tecnología de cifrado;

f) la validación de las medidas para contrarrestar las radiaciones electromagnéticas de un SIC que maneje información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior;

g) una inspección del SIC para comprobar la correcta aplicación de las medidas de seguridad documentadas.

6. Una vez cumplidos satisfactoriamente los requisitos de acreditación, la Autoridad de Acreditación de Seguridad expedirá una autorización oficial para el manejo de ICUE en la zona de acceso restringido o en el SIC, correspondiente a un grado máximo establecido de ICUE y por un período de hasta cinco años, en función del grado de ICUE manejada y de los riesgos que entrañe.

7. Tras la notificación de un fallo de seguridad o de un cambio significativo en el diseño o las medidas de seguridad de una zona de acceso restringido o de un SIC, la Autoridad de Acreditación de Seguridad revisará y, en caso necesario, podrá revocar la autorización para el manejo de ICUE hasta que se resuelvan los problemas detectados.

Artículo 5

Autoridad TEMPEST

1. A fin de proteger los SIC que manejen información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, se aplicarán medidas de seguridad TEMPEST; que, en el caso de la información clasificada de grado RESTREINT UE/EU RESTRICTE, serán facultativas.

2. La autoridad TEMPEST será la responsable de autorizar las medidas de protección adoptadas a fin de evitar que la ICUE se vea comprometida como consecuencia de emanaciones electromagnéticas no intencionadas.

3. A petición del propietario del sistema de un SIC que maneje ICUE, la autoridad TEMPEST publicará especificaciones destinadas a las medidas de seguridad TEMPEST, que se adecuarán al grado de clasificación de la información.

4. La autoridad TEMPEST realizará ensayos técnicos durante la acreditación de las zonas de acceso restringido y de los SIC para el manejo de ICUE de grado CONFIDENTIAL UE/EU CONFIDENTIAL o superior y, si se superan con éxito, expedirá un certificado TEMPEST.

5. En el certificado TEMPEST deberá constar, como mínimo:

a) la fecha de realización del ensayo;

b) una descripción de las medidas de seguridad TEMPEST, con planos de las instalaciones;

c) la fecha de expiración del certificado;

d) cualquier cambio que vaya a invalidar la certificación;

e) la firma de la autoridad TEMPEST.

6. Los LSO o los organizadores de reuniones con responsabilidad para organizar reuniones de carácter clasificado en coordinación con ellos podrán solicitar a la autoridad TEMPEST que realice ensayos en las salas de reunión para garantizar que estén protegidas técnicamente.

Artículo 6

Autoridad de Certificación Criptológica

1. La Autoridad de Certificación Criptológica será la responsable de autorizar el uso de tecnologías de cifrado.

2. La Autoridad de Certificación Criptológica publicará orientaciones sobre los requisitos para el uso y la certificación de tecnologías de cifrado.

3. La Autoridad de Certificación Criptológica certificará el uso de soluciones de cifrado a petición del propietario del sistema. La certificación se basará, como mínimo, en una evaluación satisfactoria de:

a) las necesidades de seguridad respecto de la información que debe protegerse;

b) una visión general del SIC al que se aplica la solución;

c) una evaluación de los riesgos inherentes y residuales;

d) una descripción de la solución propuesta;

e) los procedimientos operativos de seguridad para la solución de cifrado.

4. La Autoridad de Certificación Criptológica llevará un registro de las soluciones de cifrado certificadas.

Artículo 7

Autoridad de Distribución Criptológica

1. La Autoridad de Distribución Criptológica será la responsable de la distribución de los materiales criptológicos utilizados para la protección de la ICUE (principalmente, equipos de cifrado, claves criptográficas, certificados y autenticadores conexos) a:

a) los usuarios o servicios de la Comisión para los SIC administrados por terceros;

b) los usuarios u organizaciones exteriores a la Comisión para los SIC administrados por la Comisión.

2. La Autoridad de Distribución Criptológica podrá delegar en otros servicios la distribución de materiales criptológicos a terceros, de conformidad con el artículo 17, apartado 3, de la Decisión 2015/443.

3. La Autoridad de Distribución Criptológica velará por que todos los materiales criptológicos se envíen a través de canales seguros que protejan de cualquier manipulación y muestren pruebas de ella, de conformidad con las normas de seguridad aplicables al grado de clasificación de la ICUE que vaya a estar protegida por dichos materiales.

4. La Autoridad de Distribución Criptológica proporcionará orientaciones al LSO y, cuando proceda, al LISO de cada servicio de la Comisión que participe en la producción, distribución o utilización de materiales criptológicos.

5. La Autoridad de Distribución Criptológica se asegurará de que se establezcan procedimientos operativos de seguridad adecuados para el proceso de distribución.

CAPÍTULO 3

Servicios de la Comisión

Artículo 8

Jefes de Servicio

1. Cada jefe de servicio nombrará:

a) a un LSO y, en su caso, a uno o varios adjuntos, para el servicio o gabinete;

b) a un RCO y, en su caso, a uno o varios adjuntos, para cada servicio que gestione un registro de ICUE;

c) a un propietario del sistema para cada SIC que maneje ICUE.

2. El jefe de servicio solicitará la autorización del director de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad antes del nombramiento de los LSO y sus adjuntos y de los RCO y sus adjuntos.

3. El jefe de servicio identificará todos los puestos que requieran habilitación para acceder a ICUE, en consulta con el LSO. Los candidatos a tales puestos serán informados del requisito de habilitación durante el proceso de contratación.

4. El jefe de cualquier servicio que esté en posesión de ICUE tendrá la responsabilidad de activar los planes de destrucción y evacuación de emergencia en caso necesario. Los planes incluirán una alternativa para las situaciones en las que no se pueda contactar con el jefe de servicio.

Artículo 9

Propietarios del sistema de SIC que manejen ICUE

1. El propietario del sistema se pondrá en contacto con la Autoridad de Acreditación de Seguridad lo antes posible en el marco de cualquier proyecto de implantación de un SIC que maneje ICUE con el fin de determinar las normas y requisitos de seguridad pertinentes e iniciar el proceso de acreditación de seguridad.

2. El propietario del sistema velará por que las medidas de seguridad satisfagan los requisitos de la Autoridad de Acreditación de Seguridad y por que el SIC no maneje ICUE sin una acreditación previa.

3. El propietario del sistema se pondrá en contacto con la Autoridad de Certificación Criptológica a fin de obtener una certificación que le permita utilizar cualquier tecnología de cifrado. El propietario del sistema no utilizará tecnologías de cifrado en los sistemas de producción sin autorización previa.

4. El propietario del sistema consultará a los LISO del servicio en relación con las cuestiones relativas a la seguridad de los SIC.

5. El propietario del sistema revisará una vez al año, como mínimo, las medidas de seguridad que se apliquen a cualquier sistema, incluido su plan de seguridad.

6. Cuando en un SIC se produzca un incidente de seguridad que ponga de manifiesto que dicho SIC ya no está en condiciones de proteger la ICUE de forma adecuada, el propietario del sistema informará al respecto al LSO y se pondrá inmediatamente en contacto con la Autoridad de Acreditación de Seguridad para que lo asesore sobre la manera de proceder. En ese caso, se podrá suspender la acreditación e interrumpir el funcionamiento del sistema hasta que se hayan adoptado las medidas correctoras adecuadas.

7. El propietario del sistema deberá apoyar plenamente y en todo momento a la Autoridad de Acreditación de Seguridad en el desempeño de las funciones de esta relacionadas con la acreditación del SIC.

Artículo 10

Autoridad Operacional de Garantía de la Información

Corresponderá a la Autoridad Operacional de Garantía de la Información de cada SIC:

a) elaborar documentación de seguridad en consonancia con las políticas y directrices de seguridad, en particular el plan de seguridad, los procedimientos operativos de seguridad relacionados con el sistema y la documentación criptológica en el proceso de acreditación de SIC;

b) participar en la selección y ensayo de las medidas técnicas de seguridad específicas para el sistema, de los dispositivos y los programas informáticos; supervisar su aplicación y garantizar que su instalación, configuración y mantenimiento sean seguros, de conformidad con la correspondiente documentación de seguridad;

c) participar en la selección de medidas de seguridad y dispositivos TEMPEST, si así lo requiere el plan de seguridad, y, en colaboración con la autoridad TEMPEST, garantizar que su instalación y mantenimiento sean seguros;

d) supervisar el cumplimiento y la aplicación de los procedimientos operativos de seguridad relacionados con el funcionamiento del sistema;

e) gestionar y manejar productos criptológicos, en colaboración con la Autoridad de Distribución Criptológica, a fin de garantizar la custodia adecuada de los materiales criptológicos y los productos controlados y, si es preciso, garantizar la generación de variables criptológicas;

f) realizar análisis, exámenes y ensayos en materia de seguridad, en particular para elaborar los correspondientes informes sobre riesgo, cuando lo requiera la Autoridad de Acreditación de Seguridad;

g) impartir formación específica para SIC sobre la garantía de la información;

h) aplicar y ejecutar medidas de seguridad específicas para SIC.

CAPÍTULO 4

Responsable Local de Seguridad

Artículo 11

Nombramiento del Responsable Local de Seguridad

1. El responsable local de seguridad (LSO) y sus adjuntos serán funcionarios o agentes temporales.

2. Todos los LSO y sus respectivos adjuntos deberán estar en posesión de una autorización de seguridad válida para acceder a ICUE hasta de grado SECRET UE/EU SECRET, y hasta de grado TRES SECRET UE/EU TOP SECRET, cuando sea necesario. El LSO o su adjunto deberá obtener la autorización de seguridad antes de su nombramiento.

3. Las Representaciones de la Comisión podrán solicitar a la autoridad de control de la Comisión la concesión de una excepción a los requisitos establecidos en los apartados 1 y 2.

Artículo 12

Procedimientos operativos de seguridad para las zonas de acceso restringido

1. El LSO del servicio de la Comisión de que se trate elaborará procedimientos operativos de seguridad para cada zona de acceso restringido bajo su responsabilidad.

2. El LSO se asegurará de que los procedimientos operativos de seguridad incluyan los siguientes requisitos:

a) solo se permitirá el acceso sin escolta a una zona de acceso restringido en horario laboral a los miembros del personal que dispongan de una autorización de seguridad válida y justifiquen su necesidad de acceder a documentos clasificados en el grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior;

b) solo se otorgará acceso sin escolta a una zona de acceso restringido fuera del horario laboral al LSO del servicio, al o a los RCO de la zona de acceso restringido, a sus adjuntos, y al personal autorizado de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad;

c) los dispositivos de grabación y comunicación tales como los teléfonos móviles, los ordenadores, las cámaras u otros dispositivos inteligentes no estarán permitidos dentro de las zonas de acceso restringido sin una autorización previa de la CSA; cualquier excepción a esta norma deberá solicitarse con antelación a la CSA; el LSO actuará como punto de contacto;

d) tanto el personal interno como externo que necesite acceder a una zona de acceso restringido pero no cumpla los criterios establecidos en la letra a) deberá ser escoltado y vigilado en todo momento por un miembro del personal debidamente autorizado; todo acceso de estas características a una zona de acceso restringido se hará constar en un registro disponible a la entrada de esta;

e) el LSO se asegurará de que los sistemas de detección de intrusiones para la vigilancia de cualquier zona de acceso restringido estén operativos y funcionen correctamente en todo momento, y gestionará todas las contraseñas, claves, códigos PIN u otros mecanismos de acceso y autenticación;

f) las alarmas que se produzcan en una zona de acceso restringido se comunicarán a la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad, que informará inmediatamente al respecto al LSO;

g) el LSO del servicio en el que esté situada la zona de acceso restringido llevará un registro de cada intervención provocada por una alarma o un incidente de seguridad;

h) se instaurarán procedimientos para hacer frente a una alarma u otra situación de emergencia dentro de la zona de acceso restringido, incluida la evacuación del personal, que garanticen una respuesta rápida por parte de un equipo de emergencia bajo la autoridad de la CSA y de los servicios de emergencia externos, en su caso;

i) el LSO informará inmediatamente a la CSA de cualquier fallo de seguridad que se produzca dentro de una zona de acceso restringido o que la afecte, con el fin de determinar la respuesta adecuada;

j) siempre que se dejen sin vigilancia, los despachos individuales, las salas y las cajas fuertes dentro de una zona de acceso restringido deberán permanecer cerrados con llave;

k) el personal evitará toda conversación sobre información clasificada en los pasillos o en otros espacios comunes de la zona de acceso restringido cuando haya personas no autorizadas en las proximidades.

Artículo 13

Llaves y combinaciones de seguridad

1. El LSO tendrá la responsabilidad general de garantizar un manejo y depósito adecuado de las llaves y combinaciones utilizadas dentro de las zonas de acceso restringido o para acceder a ellas. Las llaves y combinaciones se depositarán en un contenedor de seguridad y dispondrán, como mínimo, del mismo nivel de protección que el material al que den acceso.

2. El LSO llevará un registro de los contenedores de seguridad y las cámaras acorazadas, junto con una lista actualizada de todos los miembros del personal que tengan acceso a ellos sin escolta.

3. El LSO llevará un registro de las llaves de los contenedores de seguridad y las cámaras acorazadas, en el que figurarán asimismo los miembros del personal a los que estén asignadas. Se conservará un recibo en relación con cada llave que se entregue, en el que constará la identificación de la llave, el destinatario, la fecha y la hora.

4. Solo tendrá conocimiento de las llaves y combinaciones el personal que las necesite y que haya obtenido la debida autorización para acceder a ICUE. El LSO recuperará cualquier llave cuando dejen de cumplirse esas condiciones.

5. El LSO tendrá bajo su custodia juegos de llaves de repuesto y un registro escrito de cada combinación en sobres individuales precintados, opacos, firmados y fechados que deberá facilitar el miembro del personal encargado de las llaves. Dichos sobres se guardarán en un contenedor de seguridad adecuado para contener el material de grado de clasificación más elevado que esté almacenado en el contenedor o sala acorazada correspondiente.

6. Si, después de un cambio de la combinación o tras la rotación de las llaves, se observan indicios de manipulación o de daños en un sobre, el LSO lo considerará un incidente de seguridad e informará inmediatamente al respecto a la CSA.

7. Los cambios de las combinaciones de los contenedores de seguridad en las zonas de acceso restringido se efectuarán bajo la supervisión del LSO. Las combinaciones se reconfigurarán, como mínimo, cada doce meses y siempre que:

a) se reciba un nuevo contenedor o se instale una nueva cerradura (en particular, se cambiarán inmediatamente las combinaciones por defecto);

b) se sospeche o se tenga la certeza de que se ha producido una situación comprometida;

c) no se requiera ya el acceso de una persona que disponga de una combinación.

8. El LSO llevará un registro de las fechas de los cambios de las combinaciones a que se refiere el apartado 7.

Artículo 14

Planes de emergencia para la evacuación y destrucción de ICUE

1. El LSO asistirá al jefe de servicio en la elaboración de planes de emergencia para la evacuación y destrucción de ICUE, sobre la base de las orientaciones facilitadas por la Dirección General de Recursos Humanos y Seguridad (HR.DS).

2. El LSO garantizará que todo el equipo necesario para la puesta en práctica de los planes previstos en el apartado 1 esté disponible de forma inmediata y se mantenga en buen estado de funcionamiento.

3. El LSO, junto con los funcionarios designados en los planes previstos en el apartado 1, revisará el estado de preparación de dichos planes, como mínimo, cada doce meses, y adoptará las medidas necesarias para actualizarlos.

Artículo 15

Autorizaciones de seguridad

1. El LSO llevará un registro de todos los puestos que, dentro del servicio, requieran una autorización de seguridad de la Comisión, así como del personal que los ocupe. El requisito de disponer de una autorización de seguridad deberá especificarse en el anuncio de vacante durante el proceso de selección y notificarse al candidato durante la entrevista.

2. El LSO supervisará todas las solicitudes de autorización de seguridad para acceder a ICUE. El LSO será el punto de contacto dentro del servicio y servirá de enlace con la CSA para la obtención de las autorizaciones de seguridad.

3. El LSO activará la solicitud de inicio del procedimiento de autorización de seguridad respecto del miembro del personal de que se trate y velará por que este devuelva sin demora el cuestionario de habilitación de seguridad nacional a la CSA.

4. El LSO garantizará que el personal del servicio con habilitación de seguridad sigue las instrucciones obligatorias sobre ICUE a fin de obtener su autorización de seguridad.

5. El LSO mantendrá contactos periódicos con el departamento de recursos humanos del servicio para obtener información sobre todos los cambios que se hayan producido en puestos que requieran una autorización de seguridad e informará inmediatamente a la autoridad de control interesada al respecto.

6. El LSO informará a la CSA de la llegada de un nuevo miembro del personal que posea ya una habilitación de seguridad para ocupar un puesto que requiera una autorización en materia de seguridad.

7. El LSO se asegurará de que los miembros del personal del servicio se sometan al procedimiento de renovación de la habilitación de seguridad en el plazo establecido. Todo miembro del personal que rehúse someterse al procedimiento estará obligado a asumir un puesto que no requiera una autorización en materia de seguridad.

Artículo 16

Registro de ICUE

1. Cuando un servicio gestione un registro de ICUE, el LSO supervisará las actividades de los RCO relativas al manejo de la ICUE y el cumplimiento de las normas de seguridad en materia de protección de la ICUE.

2. El LSO llevará a cabo los siguientes controles cada doce meses, como mínimo, y tras la sustitución de un RCO o de su adjunto:

a) el control de una muestra de documentos del registro de ICUE para confirmar el estado de los mismos y la exactitud del registro de documentos clasificados;

b) el control de una muestra de los recibos y fichas de transmisión para la distribución de ICUE al registro y desde él;

c) el control de una muestra de los certificados de destrucción.

3. Una vez al mes, como mínimo, el LSO llevará a cabo controles aleatorios del registro de documentos clasificados y de los documentos clasificados recibidos recientemente para asegurarse de que están siendo registrados de forma correcta.

4. Todos los controles quedarán registrados en el registro de documentos clasificados.

Artículo 17

Otras responsabilidades en materia de seguridad

Las demás responsabilidades en materia de seguridad del LSO se establecerán en una nota de seguridad que abarque, en particular, la seguridad física de las personas, los locales y otros activos, y la información.

CAPÍTULO 5

Controlador del Registro

Artículo 18

Nombramiento del controlador del registro

1. El controlador del registro (RCO) y sus adjuntos serán funcionarios o agentes temporales.

2. Todos los RCO y sus respectivos adjuntos deberán estar en posesión de una autorización de seguridad válida para acceder a ICUE hasta de grado SECRET UE/EU SECRET, y hasta de grado TRES SECRET UE/EU TOP SECRET, cuando sea necesario. El RCO o su adjunto deberá obtener la autorización de seguridad antes de su nombramiento.

3. Las Representaciones de la Comisión podrán solicitar a la autoridad de control de la Comisión la concesión de una excepción a los requisitos establecidos en los apartados 1 y 2.

Artículo 19

Responsabilidades

1. Los RCO registrarán la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior a efectos de seguridad:

a) cuando llegue a un servicio de la Comisión o salga de él; o

b) cuando llegue a un SIC o salga de él.

2. Los RCO registrarán todos los acontecimientos que tengan lugar durante el ciclo de vida de toda la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. Los RCO garantizarán asimismo la llevanza de un registro de toda la información clasificada de grado RESTREINT UE/EU RESTRICTED o equivalente que se intercambie con terceros países y organizaciones internacionales. Esta tarea se llevará a cabo en coordinación con el registro de ICUE gestionado por la Secretaría General.

3. El RCO registrará los documentos clasificados de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior en el registro de documentos clasificados y velará por que se almacenen de forma segura en el registro de ICUE.

4. El RCO ayudará al personal de la Comisión en la elaboración y el envío de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior.

5. Cuando los documentos clasificados con el grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se reciban de otros servicios o de terceros, el RCO velará por que el recibo de entrega sea debidamente devuelto al originador.

6. Antes de permitir que un miembro del personal acceda a un documento clasificado que obre en poder del registro de ICUE, el RCO comprobará con el LSO que el miembro del personal ha obtenido una autorización en materia de seguridad por la CSA.

7. El RCO registrará a todo el personal que se inscriba o se dé de baja en el registro de ICUE y que no esté autorizado a tener acceso sin escolta, y lo acompañará mientras dure su visita.

8. Cuando un miembro del personal extraiga del registro de ICUE un documento para su consulta, el RCO se asegurará de que esa persona tiene conocimiento de las medidas compensatorias de seguridad pertinentes y de que lo devuelve en cuanto deje de necesitarlo. El RCO recordará al personal que debe devolver todo documento de ese tipo lo antes posible.

9. El registro de ICUE expedirá un certificado de mensajería si los documentos clasificados se transportan en mano fuera del país en el que esté situado el registro.

10. Las instrucciones detalladas para los RCO sobre el registro de documentos clasificados se recogerán en una nota de seguridad.

Artículo 20

Reducción del grado de clasificación y desclasificación

El RCO asistirá a los servicios de origen en el proceso de revisión de la ICUE registrada para determinar si el grado de clasificación original sigue siendo adecuado o si el documento puede ser reclasificado en un grado inferior o desclasificado.

Artículo 21

Destrucción

1. Los RCO serán los responsables de la destrucción de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior por medios autorizados, en su caso en presencia de testigos habilitados para la seguridad.

2. Los RCO registrarán toda destrucción de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior en el registro de documentos clasificados y conservarán los certificados de destrucción correspondientes en el registro de ICUE.

Artículo 22

Tareas adicionales

1. El RCO prestará toda la asistencia necesaria al LSO cuando este lleve a cabo actividades de supervisión en el registro de ICUE.

2. El RCO informará de todo incidente de seguridad, supuesto o confirmado, al LSO, quien, a su vez, lo notificará a la CSA.

3. El RCO del registro de ICUE de un servicio de la Comisión que organice una reunión clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior preparará la ICUE que vaya a distribuirse durante la reunión y se coordinará con el organizador para garantizar que todos los documentos y recibos se manejen de conformidad con las normas pertinentes.

CAPÍTULO 6

Disposiciones finales

Artículo 23

Transparencia

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

Artículo 24

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 7 de abril de 2022.

Por la Comisión,
en nombre de la Presidenta,
Gertrud INGESTAD
Directora General
Dirección General de Recursos Humanos y Seguridad