SERVICIO EUROPEO DE ACCIÓN EXTERIOR

DECISIÓN DEL ALTO REPRESENTANTE DE LA UNIÓN PARA ASUNTOS EXTERIORES Y POLÍTICA DE SEGURIDAD

de 19 de junio de 2023,

sobre las normas de seguridad del Servicio Europeo de Acción Exterior

(2023/C 263/04)

EL ALTO REPRESENTANTE DE LA UNIÓN PARA ASUNTOS EXTERIORES Y POLÍTICA DE SEGURIDAD,

Vista la Decisión 2010/427/UE del Consejo, de 26 de julio de 2010, por la que se establece la organización y el funcionamiento del Servicio Europeo de Acción Exterior ([1]) (en lo sucesivo, «Decisión 2010/427/UE del Consejo»), y en particular su artículo 10, apartado 1,

Considerando lo siguiente:

(1) Como organismo de la Unión Europea (UE) funcionalmente autónomo, el Servicio Europeo de Acción Exterior (en lo sucesivo, «SEAE») ha de dotarse de las normas de seguridad previstas en el artículo 10, apartado 1, de la Decisión 2010/427/UE del Consejo.

(2) El Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (en lo sucesivo, «Alto Representante» o «AR») ha de adoptar para el SEAE unas normas de seguridad que cubran todos los aspectos de la seguridad por lo que respecta al funcionamiento del SEAE con el fin de que dicho organismo gestione eficazmente todos los riesgos que afecten al personal bajo su responsabilidad, a sus activos materiales, a su información y a sus visitantes, y de que ejerza su deber de diligencia y sus responsabilidades al respecto.

(3) Concretamente, debe dispensarse al personal, a los activos materiales, incluidos los sistemas de información y comunicación, a la información y a los visitantes del SEAE un nivel de protección acorde con las mejores prácticas del Consejo, la Comisión, los Estados miembros y, cuando proceda, las organizaciones internacionales.

(4) Las normas de seguridad del SEAE deben contribuir a estructurar, dentro de la Unión Europea, un marco general más completo y coherente para la protección de la información clasificada de la UE (en lo sucesivo, «ICUE»), basándose y manteniendo la mayor coherencia posible con las normas de seguridad del Consejo de la Unión Europea (en lo sucesivo, «Consejo») y con las disposiciones de la Comisión en esa misma materia.

(5) El SEAE, el Consejo y la Comisión se han comprometido a aplicar normas de seguridad equivalentes para la protección de la ICUE.

(6) La presente Decisión se entiende sin perjuicio de lo dispuesto en los artículos 15 y 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) y de los instrumentos que los desarrollan.

(7) Es preciso establecer la organización de la seguridad en el SEAE así como la asignación de las tareas de seguridad dentro de las estructuras del SEAE.

(8) El Alto Representante deberá valerse de los conocimientos especializados pertinentes de los Estados miembros, la Secretaría General del Consejo y la Comisión según lo considere necesario.

(9) El Alto Representante deberá adoptar todas las medidas necesarias para aplicar esas normas con la colaboración de los Estados miembros, la Secretaría General del Consejo y la Comisión.

([1]) DO L 201 de 3.8.2010, p. 30.

(10) Si bien el secretario general del SEAE es la Autoridad de Seguridad del SEAE, conviene revisar las normas de seguridad del SEAE, en particular para tener en cuenta la creación del Centro de Respuesta a las Crisis y, a tal efecto, derogar y sustituir la Decisión ADMIN(2017) 10 de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 19 de septiembre de 2017 ([2]).

(11) De conformidad con el artículo 15, apartado 4, letra a), de la Decisión ADMIN(2017) 10 de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 19 de septiembre de 2017, sobre las normas de seguridad del Servicio Europeo de Acción Exterior, se ha consultado al Comité de Seguridad del SEAE sobre las modificaciones previstas de las normas de seguridad del SEAE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Objetivo y ámbito de aplicación

La presente Decisión establece las normas de seguridad del Servicio Europeo de Acción Exterior (en lo sucesivo, «normas de seguridad del SEAE»).

Con arreglo al artículo 10, apartado 1, de la Decisión 2010/427/UE del Consejo, la presente Decisión será aplicable a todo el personal del SEAE y a todo el personal de las Delegaciones de la Unión, independientemente de su situación administrativa o de su origen, y establecerá el marco normativo general para la gestión efectiva de los riesgos que afecten al personal situado bajo la responsabilidad del SEAE, definido en el artículo 2, a las dependencias, a los activos materiales, a la información y a los visitantes del SEAE.

Artículo 2

Definiciones

A efectos de la presente Decisión, se entenderá por:

a) «Personal del SEAE»: los funcionarios del SEAE y otros agentes de la Unión Europea, incluidos el personal de los servicios diplomáticos de los Estados miembros contratado en calidad de agentes temporales y los expertos nacionales en comisión de servicio, tal como se definen en el artículo 6, apartados 2 y 3, de la Decisión 2010/427/UE del Consejo, respectivamente.

b) «Personal bajo la responsabilidad del SEAE»: el personal del SEAE en la sede y en las Delegaciones de la Unión y el resto del personal de las Delegaciones de la Unión, independientemente de su situación administrativa o de su origen, así como, en el contexto de la presente Decisión, el alto representante y, cuando proceda, otro personal que resida en la sede del SEAE.

c) «Personas a cargo que reúnan los requisitos»: los miembros de la familia del personal bajo la responsabilidad del SEAE en las Delegaciones de la Unión que formen parte del hogar respectivo y hayan sido notificados al Ministerio de Asuntos Exteriores del Estado receptor, y que residan efectivamente con dicho personal en el lugar de destino en el momento de la evacuación del país.

d) «Dependencias del SEAE»: todos los locales del SEAE, incluidos los edificios, oficinas, salas y otras zonas, así como los espacios que alberguen sistemas de información y comunicación (incluidos los que manejen ICUE), en los que el SEAE lleve a cabo actividades temporales o permanentes.

e) «Intereses de seguridad del SEAE»: el personal bajo la responsabilidad del SEAE, las dependencias del SEAE, las personas a cargo, los activos materiales, incluidos los sistemas de información y comunicación, la información y los visitantes.

f) «ICUE»: toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios de sus Estados miembros.

g) «Delegación de la Unión»: las delegaciones en terceros países y organizaciones internacionales contempladas en el artículo 1, apartado 4, de la Decisión 2010/427/EU del Consejo, y las oficinas de la UE de conformidad con el artículo 5 de la Decisión 2010/427/EU del Consejo.

En los anexos pertinentes y en el apéndice A se incluyen otras definiciones a efectos de la presente Decisión.

([2]) DO C 126 de 10.4.2018, p. 1.

Artículo 3

Deber de diligencia

1. Las normas de seguridad del SEAE deben tener como objetivo el ejercicio del deber de diligencia que le incumbe y sus responsabilidades al respecto.

2. El deber de diligencia del SEAE exige el ejercicio de la debida diligencia en la adopción de todas las medidas necesarias para la aplicación de medidas de seguridad dirigidas a prevenir cualquier perjuicio razonablemente previsible a sus intereses de seguridad.

Abarca tanto componentes de protección como de seguridad, incluidos los resultantes de situaciones de emergencia o crisis, cualquiera que sea su naturaleza.

3. En consideración al deber de diligencia de los Estados miembros, de las instituciones y organismos de la UE y de las otras partes que tengan personal en las Delegaciones de la Unión o en las dependencias de estas, así como el deber de diligencia del SEAE respecto de las Delegaciones de la Unión que se alojen en dependencias de las otras partes mencionadas, el SEAE suscribirá acuerdos administrativos con cada uno de los organismos anteriores, en los que se indiquen sus respectivas funciones y responsabilidades, cometidos y mecanismos de colaboración.

Artículo 4

Seguridad física y de las infraestructuras

1. El SEAE adoptará todas las medidas de seguridad física apropiadas (ya sean permanentes o temporales), incluidas las relativas al control del acceso, en todas sus dependencias, para la protección de sus intereses de seguridad. Esas medidas deberán tenerse en cuenta al proyectar y planificar nuevas dependencias o antes de arrendar las existentes.

2. Podrán imponerse obligaciones o restricciones especiales al personal bajo la responsabilidad del SEAE y a las personas a cargo, por razones de seguridad, durante un período específico y para zonas concretas.

3. Las medidas indicadas en los apartados 1 y 2 deberán ser proporcionadas al riesgo que se haya evaluado.

Artículo 5

Estados de alerta y situaciones de crisis

1. La Autoridad de Seguridad del SEAE, tal como se define en el artículo 13, sección 1, apartado 1, será responsable de definir los niveles de alerta y poner en marcha medidas de alerta adecuadas en previsión de o en respuesta a amenazas e incidentes que afecten a la seguridad del SEAE.

2. Las medidas de alerta contempladas en el apartado 1 serán acordes con el nivel de amenaza para la seguridad. La Autoridad de Seguridad del SEAE deberá definir los niveles de alerta en estrecha cooperación con los servicios competentes de otras instituciones, órganos y organismos de la Unión, y del Estado miembro o Estados miembros que acojan a los locales del SEAE.

3. La Autoridad de Seguridad del SEAE será el punto de contacto para las alertas y la respuesta a las crisis. Podrá subdelegar las tareas correspondientes, respectivamente, en el director general de Gestión de Recursos a que se refiere el artículo 4, apartado 3, letra a), segundo guion, de la Decisión 2010/427/UE del Consejo, para la sede del SEAE, y en el director del Centro de Respuesta a las Crisis para las Delegaciones de la Unión.

Artículo 6

Protección de la información clasificada

1. La protección de la ICUE se regirá por los requisitos establecidos en la presente Decisión, en particular en su anexo A. El poseedor de cualquier ICUE tendrá la responsabilidad de protegerla en consecuencia.

2. El SEAE velará por que solo se conceda acceso a la información clasificada a personas que reúnan las condiciones recogidas en el artículo 5 del anexo A.

3. El Alto Representante establecerá las condiciones para la concesión a los agentes locales de acceso a la ICUE de conformidad con las normas de protección de la ICUE establecidas en el anexo A de la presente Decisión.

4. El SEAE *garantizará la gestión de* las habilitaciones de seguridad de todo el personal bajo la responsabilidad del SEAE y de los contratistas del SEAE.

5. Cuando los Estados miembros introduzcan en las estructuras o redes del SEAE información clasificada que lleve una marca nacional de clasificación de seguridad, el SEAE protegerá dicha información con arreglo a los requisitos aplicables a la ICUE del grado equivalente, según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el apéndice B de la presente Decisión.

6. Las zonas del SEAE en las que se almacene información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL», superior o equivalente, se declararán zonas de acceso restringido conforme a las normas establecidas con arreglo al anexo A II de la presente Decisión, y serán aprobadas por la Autoridad de Seguridad del SEAE.

7. Los procedimientos para el ejercicio de las responsabilidades del Alto Representante en el marco de los acuerdos o de los acuerdos administrativos para el intercambio de ICUE celebrados con terceros Estados u organizaciones internacionales se describen en los anexos A y *A VI* de la presente Decisión.

8. El secretario general establecerá las condiciones en las que el SEAE podrá compartir ICUE que obre en su poder con otras instituciones, órganos, organismos o agencias de la Unión. Se creará un marco adecuado para ello, incluido mediante la celebración de acuerdos interinstitucionales u otros acuerdos, cuando sea necesario para tal fin.

9. Todo marco de este tipo garantizará que la ICUE reciba una protección acorde con su grado de clasificación y conforme a principios básicos y normas mínimas que sean equivalentes a los establecidos en la presente Decisión.

Artículo 7

Respuesta a incidentes, emergencias y crisis de seguridad

1. Para garantizar una respuesta a tiempo y efectiva a los incidentes de seguridad, el SEAE establecerá un procedimiento de notificación de dichos incidentes y emergencias que deberá estar operativo las 24 horas del día siete días por semana y abarcar todos los tipos de incidentes o amenazas a los intereses de seguridad del SEAE (por ejemplo, accidentes, conflictos, actos maliciosos, actos delictivos, situaciones de secuestro y toma de rehenes, emergencias médicas, incidentes en los sistemas de comunicación e información, ciberataques, etc.).

2. Deberán establecerse canales de enlace de emergencia entre la sede del SEAE, las Delegaciones de la Unión, el Consejo, la Comisión, los Representantes Especiales de la UE y los Estados miembros para ayudarles a dar respuesta a las crisis, incidentes y emergencias de seguridad que afecten al personal, así como a sus consecuencias, incluida la aplicación de planes de emergencia.

3. La respuesta a los incidentes, emergencias y crisis de seguridad implicará, entre otras cosas:

— la existencia de procedimientos de apoyo eficaz al proceso de toma de decisiones en relación con las amenazas y los incidentes y emergencias de seguridad que afecten al personal, incluida la toma de decisiones relativas a la exclusión o suspensión de una misión; y

— la existencia de una política y de procedimientos para la recuperación de personal —por ejemplo, en caso de desaparición de este o en situaciones de secuestro o toma de rehenes— teniendo en cuenta las responsabilidades específicas de los Estados miembros, de las instituciones de la UE y del SEAE. En la gestión de estas operaciones se deberá considerar la posible necesidad de capacidades específicas, en función de los recursos que puedan aportar los Estados miembros.

4. El SEAE deberá establecer los procedimientos adecuados para la notificación de los incidentes de seguridad producidos en las Delegaciones de la Unión. Cuando proceda, se deberá informar a los Estados miembros, a la Comisión, a cualquier otra autoridad relevante y a los Comités de seguridad pertinentes.

5. Los procedimientos de respuesta a incidentes, emergencias y crisis deberán someterse a ejercicios y revisiones periódicos.

Artículo 8

Seguridad de los sistemas de comunicación e información

1. EL SEAE protegerá la información que se maneje a través de los sistemas de información y comunicación (en lo sucesivo, «SIC»), en el sentido definido en el apéndice A de la presente Decisión, frente a toda amenaza que comprometa su confidencialidad, integridad, disponibilidad, autenticidad e irrenunciabilidad.

2. La Autoridad de Seguridad del SEAE deberá aprobar las normas, las directrices de seguridad y el programa de seguridad para la protección de todos los SIC propiedad del SEAE.

3. Dichas normas, directrices y programa deberán ser conformes con los del Consejo y la Comisión, y su aplicación deberá coordinarse estrechamente con ellas y, cuando proceda, con las políticas de seguridad aplicadas por los Estados miembros.

4. Todo SIC que maneje información clasificada deberá ser sometido a un proceso de acreditación. EL SEAE aplicará un sistema de acreditación de la seguridad previa consulta con la Secretaría General del Consejo y con la Comisión.

5. Cuando la protección de la ICUE manejada por el SEAE se realice a través de productos criptográficos, estos productos deberán ser aprobados por la Autoridad de Autorización Criptológica del SEAE previa recomendación del Comité de Seguridad del Consejo.

6. La Autoridad de Seguridad del SEAE deberá establecer, en la medida necesaria, las siguientes funciones respecto de la garantía de la información:

a) una Autoridad de Garantía de la Información (AGI);

b) una Autoridad TEMPEST;

c) una Autoridad de Certificación Criptológica (ACC);

d) una Autoridad de Distribución Criptológica (ADC).

7. Para cada sistema, la Autoridad de Seguridad del SEAE determinará las siguientes funciones:

a) una Autoridad de Acreditación de Seguridad (AAS);

b) una Autoridad Operativa de Garantía de la Información (AOGI).

8. Las disposiciones para la aplicación de este artículo en relación con la protección de la ICUE se establecen en los anexos A y A IV.

Artículo 9

Fallos en la seguridad y comprometimientos de la información clasificada

1. Se produce un fallo en la seguridad a resultas de una acción u omisión contraria a las normas de seguridad establecidas en la presente Decisión o a las políticas o directrices de seguridad que recojan las medidas necesarias para su aplicación, aprobadas de conformidad con el artículo 21, apartado 1.

2. Se produce un comprometimiento de la información clasificada cuando se revela esta, en su totalidad o en parte, a personas o entidades no autorizadas.

3. Todo fallo o sospecha de fallo en la seguridad y todo comprometimiento o sospecha de comprometimiento de la información clasificada deberá notificarse inmediatamente al director encargado de la seguridad de la sede y la seguridad de la información del SEAE, que adoptará las medidas adecuadas, tal como se establecen en el anexo A, artículo 11.

4. Toda persona que sea responsable de un fallo en la seguridad por incumplimiento de las normas establecidas en la presente Decisión o de exponer a comprometimiento información clasificada estará sujeta a medidas disciplinarias o legales de conformidad con las disposiciones legales, normativas y reglamentarias aplicables, de conformidad con el artículo 11, apartado 3, del anexo A.

Artículo 10

Investigación de incidentes, fallos o comprometimientos de la seguridad y acciones correctivas

1. Sin perjuicio de lo dispuesto en el artículo 86 y el anexo IX del Estatuto de los funcionarios ([3]), la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE podrá iniciar y realizar investigaciones de seguridad:

a) en caso de posibles fugas, mal manejo o comprometimientos de ICUE, de información clasificada de Euratom o de información delicada no clasificada;

b) para contrarrestar ataques de servicios de inteligencia hostiles contra el SEAE y su personal;

c) para contrarrestar atentados terroristas contra el SEAE y su personal;

d) en caso de ciberincidentes;

e) en caso de otros incidentes que afecten o puedan afectar a la seguridad general en el SEAE, incluida la sospecha de infracciones penales.

2. La Autoridad de Seguridad del SEAE, asistida por la Dirección encargada de la seguridad de la sede [...] y la seguridad de la información del SEAE, la Dirección encargada del Centro de Respuesta a las Crisis y los expertos de los Estados miembros o de otras instituciones de la UE, según proceda, deberá aplicar las acciones correctivas que sean precisas de resultas de una investigación, en el momento y forma que sean apropiados.

Únicamente el personal autorizado en virtud de un mandato nominativo conferido por la Autoridad de Seguridad del SEAE, habida cuenta de sus funciones, tendrá la facultad de coordinar y realizar investigaciones de seguridad en el SEAE.

3. Para la realización de dichas investigaciones, los investigadores tendrán acceso a toda la información necesaria y contarán al respecto con el pleno apoyo de todo el personal y servicios del SEAE.

Los investigadores podrán adoptar medidas adecuadas para proteger el rastro de las pruebas de un modo proporcionado a la gravedad del asunto investigado.

4. Cuando el acceso a la información implique datos personales, incluidos los contenidos en los sistemas de información y comunicación, dicho acceso se tratará de conformidad con lo previsto en el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([4]).

5. Cuando sea necesario crear una base de datos de investigación que contenga datos personales, se notificará al Supervisor Europeo de Protección de Datos (SEPD), de conformidad con el Reglamento mencionado.

Artículo 11

Gestión del riesgo de seguridad

1. A fin de determinar las necesidades de protección de la seguridad del SEAE, la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y la Dirección encargada del Centro de Respuesta a las Crisis elaborarán y mantendrán actualizada una metodología global de evaluación de los riesgos para la seguridad, en estrecha cooperación con la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión y, cuando proceda, con la Dirección de Prevención y Seguridad de la Secretaría General del Consejo.

2. Los riesgos para los intereses de seguridad del SEAE se gestionarán en forma de proceso. El objetivo de ese proceso será determinar los riesgos conocidos para la seguridad, definir las medidas de seguridad dirigidas a reducirlos hasta niveles aceptables y aplicar disposiciones acordes con el concepto de defensa en profundidad. La eficacia de dichas medidas, y el nivel de riesgo, serán objeto de una evaluación continua.

([3]) Estatuto de los funcionarios de la Unión Europea y régimen aplicable a los otros agentes de la Unión Europea, en lo sucesivo «Estatuto de los funcionarios»

([4]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas jurídicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos (DO L 295 de 21.11.2018, p. 39).

3. Las funciones, responsabilidades y cometidos que establece la presente Decisión se entienden sin perjuicio de la responsabilidad de cada miembro del personal bajo la responsabilidad del SEAE; en particular, el personal de la UE en misión en terceros países deberá ejercer el sentido común y el buen juicio respecto de su propia protección y seguridad, y cumplir todas las normas, reglamentos, procedimientos e instrucciones de seguridad.

4. Con el fin de prevenir y controlar los riesgos para la seguridad, el personal autorizado podrá llevar a cabo comprobaciones de los antecedentes personales de las personas comprendidas en el ámbito de aplicación de la presente Decisión, con el fin de determinar si facilitar a dichas personas el acceso a los locales o información del SEAE representa una amenaza para la seguridad. Con este fin, y de conformidad con el Reglamento (UE) 2018/1725, el personal autorizado en cuestión podrá: a) utilizar cualquier fuente de información de que disponga el SEAE, teniendo en cuenta la fiabilidad de la fuente de información; b) acceder al expediente o los datos que posea el SEAE respecto de las personas que emplea, o pretende emplear, o del personal de los contratistas cuando esté debidamente justificado.

5. EL SEAE adoptará todas las medidas oportunas para garantizar la protección de sus intereses de seguridad y para impedir cualquier daño racionalmente previsible que aquellos pudieren sufrir.

6. Las medidas de seguridad aplicadas en el SEAE con miras a la protección de la ICUE a lo largo de todo su ciclo de vida serán proporcionales a su nivel de clasificación de seguridad, a la forma y el volumen de la información o el material, a la ubicación o la construcción de las instalaciones que contengan la ICUE y a las amenazas —incluso las evaluadas de forma local— de actividades dolosas o delictivas como el espionaje, el sabotaje y el terrorismo.

Artículo 12

Formación y concienciación en cuestiones de seguridad

1. La Autoridad de Seguridad del SEAE velará por que la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE elabore programas adecuados de formación y concienciación en cuestiones de seguridad. El personal de la sede recibirá las sesiones informativas y la formación necesarias de concienciación en cuestiones de seguridad, que impartirán los equipos de concienciación en cuestiones de seguridad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE. El personal de las Delegaciones de la Unión y, cuando proceda, las personas a cargo que reúnan los requisitos, asistirán a las sesiones informativas y a las actividades de formación y concienciación en cuestiones de seguridad acordes con los riesgos existentes en su lugar de trabajo o de residencia, que impartirán los equipos de gestión de la seguridad en coordinación con la Dirección encargada del Centro de Respuesta a las Crisis.

2. Antes de recibir acceso a la ICUE y, posteriormente, a intervalos regulares, el personal deberá ser instruido acerca de sus responsabilidades en materia de protección de la ICUE y aceptar esas responsabilidades de acuerdo con las normas establecidas conforme al artículo 6.

Artículo 13

Organización de la seguridad en el SEAE

Sección 1 Disposiciones generales

1. El secretario general será la Autoridad de Seguridad del SEAE. En tal calidad, el secretario general se asegurará de que:

a) las medidas de seguridad se coordinen en la medida necesaria con las autoridades competentes de los Estados miembros, la Secretaría General del Consejo y la Comisión y, cuando proceda, con terceros países u organizaciones internacionales, en lo tocante a todos los aspectos de la seguridad pertinentes para las actividades del SEAE, incluida la naturaleza de los riesgos para los intereses de seguridad del SEAE y los medios de protección frente a estos;

b) los aspectos de seguridad se tengan plenamente en cuenta desde el inicio de cualesquiera de las actividades del SEAE;

c) solo se conceda acceso a la información clasificada a personas que reúnan las condiciones establecidas en el artículo 5 del anexo A;

d) se adopten las medidas adecuadas para gestionar las habilitaciones de seguridad de todo el personal bajo la responsabilidad del SEAE y de los contratistas del SEAE;

e) se establezca un sistema de registro para garantizar que toda la información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior se maneje conforme a la presente Decisión, tanto dentro del SEAE como en caso de divulgación a Estados miembros, instituciones, órganos u organismos de la UE o a otros receptores autorizados. Deberá llevarse un registro separado de toda la ICUE divulgada por el SEAE a terceros países u organizaciones internacionales y de toda la información clasificada recibida de terceros países u organizaciones internacionales;

f) se efectúen las inspecciones de seguridad contempladas en el artículo 16;

g) se efectúen investigaciones en relación con todo fallo o sospecha de fallo en la seguridad, así como sobre cualquier comprometimiento real o sospecha comprometimiento o pérdida de información clasificada que obre en poder o proceda del SEAE, y se solicite a las autoridades de seguridad competentes asistencia para dichas investigaciones;

h) se establezcan los planes y mecanismos apropiados de gestión de los incidentes y sus consecuencias, con el fin de reaccionar de forma oportuna y eficaz ante los incidentes de seguridad;

i) se adopten las medidas adecuadas en caso de incumplimiento de la presente Decisión por parte de personas físicas;

j) se hayan dispuesto las medidas físicas y organizativas necesarias para la protección de los intereses de seguridad del SEAE.

A este respecto, la Autoridad de Seguridad del SEAE:

— establecerá la categoría de seguridad de las Delegaciones de la Unión, en consulta con la Comisión;

— establecerá un mecanismo de respuesta a las crisis y definirá sus tareas y responsabilidades;

— decidirá, previa consulta al AR, en su caso, cuándo se debe evacuar al personal de la Delegación de la Unión si la situación en materia de seguridad lo requiere;

— decidirá las medidas que deban aplicarse para la protección de las personas a cargo que reúnan los requisitos, cuando proceda, teniendo en cuenta los acuerdos celebrados con las instituciones de la UE contemplados en el artículo 3, apartado 3;

— aprobará la política de comunicación criptológica, en particular el programa de instalación de productos y mecanismos criptográficos.

2. De conformidad con el artículo 10, apartado 3, de la Decisión 2010/427/UE del Consejo, la Autoridad de Seguridad del SEAE estará asistida en estas tareas conjuntamente por:

i) el director general de Gestión de Recursos, asistido por el director encargado de la seguridad de la sede y la seguridad de la información del SEAE;

ii) el director del Centro de Respuesta a las Crisis;

y, cuando proceda, por el secretario general adjunto de Paz, Seguridad y Defensa, con el fin de garantizar la coherencia con las medidas de seguridad que deban adoptarse para las misiones y operaciones de la PCSD.

3. El secretario general, como Autoridad de Seguridad del SEAE, podrá subdelegar sus tareas, cuando proceda.

4. Cada jefe de departamento o división será responsable de garantizar la aplicación de dichas normas, así como de las directrices de seguridad a que se refiere el artículo 21 de la presente Decisión y de cualquier otro procedimiento o medida de protección de la ICUE dentro de su departamento o división.

Sin perjuicio de asumir su responsabilidad tal como se ha indicado, cada jefe de departamento o división nombrará a miembros del personal para el puesto de coordinador de seguridad. El número de miembros del personal en dicho puesto será acorde con el volumen de ICUE que maneje el departamento o división.

Cuando proceda, los coordinadores de seguridad asistirán y apoyarán al jefe del departamento o división en el desempeño de las tareas relacionadas con la seguridad, como:

a) la elaboración de los requisitos de seguridad adicionales que requieran las necesidades específicas del departamento o división, en consulta con la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE;

b) la complementación de las sesiones informativas periódicas en materia de seguridad organizadas por la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE para los miembros del departamento o división sobre los requisitos de seguridad adicionales a que se refiere la letra a);

c) la garantía de la observancia del principio de «necesidad de conocer» en el departamento o división;

d) la actualización de la lista de claves y códigos seguros, cuando proceda;

e) la garantía de que, cuando proceda, los procedimientos y medidas de seguridad estén actualizados y sean eficaces;

f) la comunicación de cualquier fallo en la seguridad o comprometimiento de la ICUE tanto al director como a la Dirección encargados de la seguridad de la sede y la seguridad de la información del SEAE;

g) la organización de sesiones informativas finales para el personal que deje de estar empleado por el SEAE;

h) la presentación de informes periódicos a sus superiores sobre los asuntos de seguridad del departamento o división;

i) el mantenimiento de contactos con la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE sobre cuestiones de seguridad.

Deberá ser oportunamente notificada a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE toda actividad o asunto que pueda repercutir en la seguridad.

Sección 2 Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE

1. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE se enmarcará administrativamente en la Dirección General de Gestión de Recursos. Esta deberá:

a) ejercer el deber de diligencia del SEAE en la sede del SEAE y encargarse de todas las cuestiones de seguridad de la sede del SEAE, en particular en lo que respecta a los sistemas de información y comunicación (SIC) y la seguridad de la información para las Delegaciones de la Unión;

b) gestionar, coordinar, supervisar o aplicar todas las medidas de seguridad en las dependencias de la sede del SEAE.

c) velar por la coherencia y congruencia con la presente Decisión y con sus disposiciones de aplicación de cualquier actividad que repercuta en la protección de los intereses de seguridad del SEAE;

d) apoyar las actividades de la Autoridad de Acreditación de Seguridad del SEAE realizando evaluaciones físicas de la seguridad del entorno general de seguridad (EGS) y el entorno local de seguridad (ELS) de los sistemas de información y comunicación que manejen ICUE, y de las dependencias del SEAE autorizadas para manejar y almacenar ICUE.

La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE estará asistida por los servicios competentes de los Estados miembros, de conformidad con el artículo 10, apartado 3, de la Decisión 2010/427/UE del Consejo.

2. El director encargado de la seguridad de la sede y la seguridad de la información del SEAE será responsable de:

a) garantizar la protección global de los intereses de seguridad del SEAE en el ámbito de responsabilidad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE;

b) redactar, revisar y actualizar las normas de seguridad, así como las medidas de coordinación de la seguridad con el director del Centro de Respuesta a las Crisis, las autoridades competentes de los Estados miembros y, si procede, de terceros Estados y organizaciones internacionales vinculados a la UE por acuerdos o convenios en materia de seguridad;

c) actuar como asesor principal del AR, de la Autoridad de Seguridad del SEAE y del secretario general adjunto de Paz, Seguridad y Defensa en todos los asuntos relacionados con la seguridad de la sede y la seguridad de la información del SEAE;

d) gestionar las habilitaciones de seguridad de todo el personal bajo la responsabilidad del SEAE y de los contratistas del SEAE;

e) presidir el Comité de Seguridad del SEAE en su formación de autoridades nacionales de seguridad (ANS), tal como se establece en el artículo 15, apartado 1, de la presente Decisión, siguiendo instrucciones de la Autoridad de Seguridad del SEAE, y apoyar sus procedimientos;

f) mantener contactos con cualesquiera socios o autoridades distintos de los contemplados en la letra b) anterior sobre asuntos de seguridad en el ámbito de responsabilidad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE;

g) establecer prioridades y presentar propuestas para la gestión del presupuesto de seguridad en la sede y en las Delegaciones de la Unión, esta última en coordinación con el director del Centro de Respuesta a las Crisis.

h) velar por que se registren los fallos de seguridad y comprometimientos a que se refiere el artículo 9 de la presente Decisión y se inicien y lleven a cabo investigaciones en los casos necesarios;

i) reunirse periódicamente y siempre que sea necesario para debatir asuntos de interés común con el director de Seguridad de la Secretaría General del Consejo y el director de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión.

3. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE establecerá contacto y mantendrá una estrecha colaboración en su ámbito de responsabilidad con:

— las Autoridades Nacionales de Seguridad (ANS) u otras autoridades competentes en materia de seguridad de los Estados miembros, para que le asistan en relación con la información necesaria para evaluar los peligros y amenazas para el SEAE, su personal, sus actividades, sus activos y recursos y su información clasificada en su lugar habitual de actividad;

— las autoridades competentes en materia de seguridad de los terceros Estados con los que la UE haya celebrado un acuerdo de seguridad de la información, o en cuyo territorio la Unión haya desplegado una misión u operación de la PCSD; la Oficina de Seguridad de la Secretaría General del Consejo y la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión y, cuando proceda, los servicios de seguridad de otras instituciones, órganos y organismos de la UE;

— los servicios de seguridad de las organizaciones internacionales con las que la UE haya celebrado un acuerdo de seguridad de la información; y

— las ANS de los Estados miembros, sobre cualquier cuestión relacionada con la protección de ICUE, en particular sobre las habilitaciones personales de seguridad.

Sección 3 Dirección encargada del Centro de Respuesta a las Crisis

1. La Dirección encargada del Centro de Respuesta a las Crisis deberá:

a) ejercer el deber de diligencia del SEAE en las Delegaciones de la Unión;

b) garantizar diariamente la seguridad del personal bajo la responsabilidad del SEAE en las Delegaciones de la Unión, proponer las medidas que deben adoptarse en caso de crisis para garantizar la continuidad de las actividades en las Delegaciones de la Unión y aplicar los procedimientos de evacuación en estrecha coordinación con la División de Coordinación de la Dirección General de Gestión de Recursos;

c) gestionar, coordinar, supervisar o aplicar todas las medidas de seguridad en las dependencias del SEAE en las Delegaciones de la Unión;

d) velar por la coherencia y congruencia con la presente Decisión y con sus disposiciones de aplicación de cualquier actividad del SEAE que repercuta en los intereses de seguridad del SEAE en el ámbito de responsabilidad del Centro de Respuesta a las Crisis;

e) apoyar las actividades de la Autoridad de Acreditación de Seguridad del SEAE realizando las evaluaciones de seguridad física de las dependencias de las Delegaciones de la Unión autorizadas para manejar y almacenar ICUE;

2. El director encargado del Centro de Respuesta a las Crisis será responsable de:

a) garantizar la protección global de los intereses de seguridad del SEAE en el ámbito de responsabilidad de la Dirección encargada del Centro de Respuesta a las Crisis;

b) coordinar las medidas y procedimientos de seguridad con las autoridades competentes de los Estados de acogida y, cuando proceda, con las organizaciones internacionales pertinentes;

c) garantizar la activación y gestión del Mecanismo de Respuesta a las Crisis del SEAE;

d) diseñar y gestionar la capacidad de despliegue del SEAE (equipo de apoyo al despliegue, incluido el equipamiento necesario) y garantizar su disponibilidad en todo momento;

e) actuar como asesor principal del AR, de la Autoridad de Seguridad del SEAE y del secretario general adjunto de Paz, Seguridad y Defensa en todos los asuntos relacionados con la seguridad en las Delegaciones de la Unión y en la respuesta a las crisis que les afectan;

f) presidir el Comité de Seguridad del SEAE en su formación de ministros de Asuntos Exteriores, tal como se establece en el artículo 15, apartado 1, de la presente Decisión, siguiendo instrucciones de la Autoridad de Seguridad del SEAE, y apoyar sus procedimientos;

g) mantener contactos con cualesquiera socios o autoridades distintos de los contemplados en la letra b) anterior sobre asuntos de seguridad en el ámbito de responsabilidad de la Dirección encargada del Centro de Respuesta a las Crisis;

h) contribuir a establecer prioridades y presentar propuestas para la gestión del presupuesto destinado a la seguridad en las Delegaciones de la Unión, coordinado por el director encargado de la seguridad de la sede y la seguridad de la información del SEAE.

i) garantizar que los fallos de seguridad y comprometimientos en el ámbito de responsabilidad de la Dirección encargada del Centro de Respuesta a las Crisis se notifiquen a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE para que reciban el seguimiento adecuado;

3. La Dirección encargada del Centro de Respuesta a las Crisis establecerá contacto y mantendrá una estrecha colaboración en su ámbito de responsabilidad con:

— los departamentos pertinentes de los ministerios de Asuntos Exteriores de los Estados miembros;

— en la medida en que sea necesario, las autoridades competentes en materia de seguridad de los Estados de acogida en cuyo territorio estén establecidas las Delegaciones de la UE, en lo que respecta a los intereses de seguridad del SEAE;

— la Oficina de Seguridad de la Secretaría General del Consejo y la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión y, cuando proceda, los servicios de seguridad de otras instituciones, órganos y organismos de la UE, en sus ámbitos de responsabilidad;

— los servicios de seguridad de las organizaciones internacionales, con vistas a una coordinación útil, en su ámbito de responsabilidad.

Sección 4 Delegaciones de la Unión

1. Cada jefe de Delegación será responsable de la aplicación y la gestión local de todas las medidas de protección de los intereses de seguridad del SEAE en las dependencias de dicha Delegación y en su ámbito de responsabilidad.

Bajo la orientación del Centro de Respuesta a las Crisis y en consulta con las autoridades competentes del Estado de acogida adoptará, cuando sea necesario, medidas razonablemente viables para garantizar la aplicación de las medidas físicas y organizativas adecuadas para ejercer su deber de diligencia.

El jefe de Delegación deberá redactar protocolos de seguridad para la protección de las personas a cargo que cumplan los requisitos, tal como se definen en el artículo 2, letra c), cuando proceda, teniendo en cuenta cualquier acuerdo administrativo que se haya celebrado, tal como se indica en el artículo 3, apartado 3.

El jefe de Delegación informará de todas las cuestiones relacionadas con el deber de diligencia que sean de su competencia al director de la Dirección encargada del Centro de Respuesta a las Crisis, y al director de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE de las relacionadas con otras cuestiones de seguridad.

Le asistirán la Dirección encargada del Centro de Respuesta a las Crisis, el equipo de gestión de la seguridad de la Delegación de la Unión, que se compone de personal que ejerce las tareas y funciones de seguridad, y, cuando sea necesario, el personal de seguridad. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE prestará asistencia en su ámbito de responsabilidad.

La Delegación de la Unión mantendrá contactos regulares y una estrecha colaboración en materia de seguridad con las misiones diplomáticas de los Estados miembros.

2. Además, el jefe de Delegación:

— establecerá, en coordinación con el Centro de Respuesta a las Crisis, planes detallados de emergencia y seguridad de la Delegación de la Unión, basados en procedimientos operativos normalizados;

— mantendrá un sistema efectivo (24 horas al día los siete días de la semana) de gestión de los incidentes y emergencias de seguridad dentro del ámbito de actividad de la Delegación de la Unión;

— velará por que todo el personal desplegado en la Delegación de la Unión esté cubierto por un seguro, tal como requieran las condiciones en la zona;

— velará por que la seguridad forme parte de la formación introductoria que se imparta a todo el personal desplegado en la Delegación de la Unión con anterioridad o simultáneamente a su llegada a esta; y

— velará por que se apliquen las recomendaciones formuladas de resultas de las evaluaciones de seguridad, y presentará periódicamente informes escritos sobre su aplicación al director encargado del Centro de Respuesta a las Crisis y al director encargado de la seguridad de la sede y la seguridad de la información del SEAE.

3. El jefe de la Delegación, sin perjuicio de asumir la responsabilidad y tener que rendir cuentas por la gestión de la seguridad, así como de velar por la resiliencia de la organización, podrá delegar la ejecución de sus tareas de seguridad en el coordinador de seguridad de la Delegación («CSD»), que será el jefe adjunto de la Delegación o, si no se ha nombrado a nadie, en un suplente adecuado.

En particular, podrán delegarse las siguientes responsabilidades:

— coordinar las funciones de seguridad en las Delegaciones de la Unión;

— mantener contactos sobre temas de seguridad con las autoridades competentes del Estado de acogida y los homólogos adecuados en las embajadas y misiones diplomáticas de los Estados miembros;

— aplicar procedimientos adecuados de gestión de la seguridad en relación con los intereses de seguridad del SEAE, incluida la protección de la ICUE;

— velar por el cumplimiento de las normas e instrucciones de seguridad;

— instruir al personal en las normas de seguridad que le sean aplicables y en los riesgos específicos existentes en el Estado de acogida;

— presentar a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE solicitudes de habilitaciones de seguridad y relativas a los puestos que requieran una habilitación personal de seguridad; y y

— mantener permanentemente informados al jefe de la Delegación, al responsable regional de seguridad (RRS) y a la Dirección encargada del Centro de Respuesta a las Crisis sobre incidentes o sucesos en materia de seguridad en la zona que incidan en la protección de los intereses de seguridad del SEAE.

4. El jefe de la Delegación podrá delegar tareas de seguridad de carácter técnico o administrativo en el jefe de Administración o en otros miembros del personal de la Delegación de la Unión.

5. Las Delegaciones de la Unión contarán con la asistencia de un RRS. El RRS desempeñará las funciones definidas a continuación en las Delegaciones de la Unión en sus respectivas zonas geográficas de responsabilidad.

En determinadas circunstancias, cuando la situación en materia de seguridad así lo dicte, se podrá asignar un RRS exclusivo a una Delegación de la Unión específica como residente a tiempo completo.

Se podrá pedir a un RRS que se traslade a una zona situada fuera de su zona de responsabilidad, incluida la sede, o incluso que ocupe un puesto de residente en función de la situación de seguridad en un determinado país, tal como lo solicite la Dirección encargada del Centro de Respuesta a las Crisis.

6. Los RRS estarán bajo el control operativo directo del servicio de la sede del SEAE encargado de la seguridad sobre el terreno, pero bajo el control administrativo compartido del jefe de Delegación de su lugar de destino y del servicio de la sede encargado de la seguridad sobre el terreno. Asesorarán y asistirán al jefe y al personal de la Delegación de la Unión en la adopción y aplicación de todas las medidas físicas, organizativas y de procedimiento relacionadas con la seguridad de la Delegación de la Unión.

7. Los RRS prestarán asesoramiento y apoyo al jefe y al personal de la Delegación de la Unión. Cuando proceda, en particular cuando un RRS sea residente a tiempo completo, deberá asistir a la Delegación de la Unión en la gestión y aplicación de la seguridad, incluida la preparación de contratos en materia de seguridad y la gestión de acreditaciones y habilitaciones.

Artículo 14

Operaciones PCSD y representantes especiales de la UE

El director encargado de la seguridad de la sede y la seguridad de la información del SEAE y el director encargado del Centro de Respuesta a las Crisis asesorarán, dentro de los respectivos ámbitos de responsabilidad de sus Direcciones y cuando sea necesario, al director ejecutivo de política común de seguridad y defensa (PCSD), al director general del Estado Mayor de la Unión Europea (EMUE), también en su calidad de director de la Capacidad Militar de Planificación y Ejecución, y al director ejecutivo de la Capacidad Civil de Planeamiento y Ejecución (CPCC) sobre los aspectos relacionados con la seguridad del planeamiento y la ejecución de las misiones y operaciones de la PCSD, y a los representantes especiales de la UE sobre los aspectos de seguridad de su mandato, de forma complementaria a las disposiciones específicas al respecto recogidas en las políticas pertinentes adoptadas por el Consejo.

Artículo 15

Comité de Seguridad del SEAE

1. Se crea un Comité de Seguridad del SEAE.

Dicho Comité estará presidido por la Autoridad de Seguridad del SEAE o un delegado designado y se reunirá de conformidad con las instrucciones del presidente o a petición de cualquiera de sus miembros. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y la Dirección encargada del Centro de Respuesta a las Crisis apoyarán al presidente en sus funciones, dentro de sus respectivos ámbitos de responsabilidad, y, en caso necesario, prestarán asistencia administrativa a los trabajos del Comité.

2. El Comité de Seguridad del SEAE estará compuesto por representantes de:

— cada Estado miembro;

— la Oficina de Seguridad de la Secretaría General del Consejo;

— la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión.

La delegación de un Estado miembro en el Comité de Seguridad del SEAE podrá estar integrada por miembros de:

— la Autoridad Nacional de Seguridad (ANS) o la Autoridad de Seguridad Designada (ASD),

— los servicios encargados de la seguridad en los Ministerios de Asuntos Exteriores.

3. Los representantes del Comité podrán ser acompañados y asesorados por expertos si lo estiman necesario. Se podrá invitar a representantes de otras instituciones, órganos y organismos de la UE cuando se debatan cuestiones relevantes para su seguridad.

4. Sin perjuicio de lo dispuesto en el apartado 5 siguiente, el Comité de Seguridad del SEAE asistirá al SEAE, mediante consulta, en todos los asuntos de seguridad relevantes para las actividades del SEAE, su sede y las Delegaciones de la Unión.

En particular, sin perjuicio de lo dispuesto en el apartado 5 siguiente, el Comité de Seguridad del SEAE:

a) será consultado sobre:

   — los conceptos, directrices y políticas de seguridad u otros documentos metodológicos relacionados con la seguridad, en especial por lo que respecta a la protección de la información clasificada y las medidas que deben adoptarse en caso de que el personal del SEAE infrinja las normas de seguridad;

   — los aspectos técnicos de la seguridad que puedan influir en la decisión del AR de presentar una recomendación al Consejo para la apertura de las negociaciones de los acuerdos de seguridad de la información contemplados en el artículo 10, apartado 1, letra a), del anexo A;

   — cualquier modificación de la presente Decisión;

b) podrá ser consultado o informado, según proceda, sobre asuntos relacionados con la seguridad del personal y los activos de la sede del SEAE y las Delegaciones de la Unión, sin perjuicio de lo dispuesto en el artículo 3, apartado 3;

c) será informado de cualquier comprometimiento o pérdida de ICUE que se produzca en el SEAE.

5. Cualquier cambio en las normas de protección de la ICUE contenidas en la presente Decisión y en su anexo A requerirá el dictamen favorable y unánime de los Estados miembros representados en el Comité de Seguridad del SEAE. También se requerirá dicho dictamen favorable y unánime antes de:

— iniciar las negociaciones de los acuerdos administrativos contemplados en el artículo 10, apartado 1, letra b) del anexo A;

— revelar información clasificada en las circunstancias excepcionales indicadas en los puntos 9, 11 y 12 del anexo A VI;

— asumir la responsabilidad del originador de la información en las circunstancias contempladas en el artículo 10, apartado 6, última frase, del anexo A.

En los casos en que se requiera un dictamen favorable y unánime, se cumplirá esta condición cuando las delegaciones de los Estados miembros no expresen objeciones durante los trabajos del Comité.

6. El Comité de Seguridad del SEAE tendrá plenamente en cuenta las directrices y políticas de seguridad vigentes en el Consejo y la Comisión.

7. El Comité de Seguridad del SEAE recibirá la lista de las inspecciones anuales del SEAE, una vez finalizadas, junto con los informes de estas.

8. Organización de las reuniones:

— El Comité de Seguridad del SEAE se reunirá al menos dos veces al año. El presidente podrá convocar reuniones adicionales, bien en su configuración completa o en el formato de seguridad ANS/ASD o MAE (Ministerios de Asuntos Exteriores). Dichas reuniones también podrán ser solicitadas por los miembros del Comité.

— El Comité de Seguridad del SEAE organizará sus actividades de manera que pueda formular recomendaciones sobre aspectos específicos de la seguridad. En caso necesario, podrá establecer otras subsecciones de expertos. Elaborará mandatos para dichas subsecciones y recibirá informes de sus actividades.

— La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y la Dirección encargada del Centro de Respuesta a las Crisis serán responsables de preparar los temas de debate en sus respectivos ámbitos de responsabilidad. El presidente establecerá el orden del día provisional de cada sesión. Los miembros del Comité podrán proponer temas adicionales de debate.

Artículo 16

Inspecciones de seguridad

1. La Autoridad de Seguridad del SEAE velará por que se realicen inspecciones de seguridad, de forma periódica, en la sede del SEAE y en las Delegaciones de la Unión para evaluar la adecuación de la aplicación de las medidas de seguridad y comprobar que cumplen la presente Decisión. Cuando proceda, la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, en cooperación con la Dirección encargada del Centro de Respuesta a las Crisis, podrá designar expertos colaboradores para participar en inspecciones de seguridad en los órganos y organismos de la UE establecidos en virtud del título V, capítulo 2, del TUE.

2. Las inspecciones de seguridad del SEAE se efectuarán bajo la autoridad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, con el apoyo de la Dirección encargada del Centro de Respuesta a las Crisis cuando proceda, y, en el contexto de los acuerdos contemplados en el artículo 3, apartado 3, con el apoyo de expertos en seguridad que representen a otras instituciones de la UE o Estados miembros.

3. El SEAE podrá recurrir, en la medida necesaria, a los conocimientos especializados de los Estados miembros, la Secretaría General del Consejo y la Comisión Europea.

Cuando sea necesario, se podrá invitar a participar en la inspección de seguridad de una Delegación de la Unión a expertos en seguridad de las misiones diplomáticas de los Estados miembros en terceros países o a representantes de los servicios diplomáticos de seguridad de los Estados miembros.

4. Las disposiciones para la aplicación del presente artículo en relación con la protección de la ICUE se establecen en el anexo A III.

Artículo 17

Visitas de evaluación

Se organizarán visitas de evaluación para determinar la efectividad de las medidas de seguridad establecidas en un tercer Estado u organización internacional con miras a proteger la ICUE intercambiada al amparo de un acuerdo administrativo contemplado en el artículo 10, apartado 1, letra b), del anexo A.

La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE podrá designar expertos colaboradores para que participen en las visitas de evaluación a terceros Estados u organizaciones internacionales con los que la UE haya celebrado un acuerdo de seguridad de la información, tal como se contempla en el artículo 10, apartado 1, letra a), del anexo A.

Artículo 18

Planificación de la continuidad de las actividades

La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y la Dirección encargada del Centro de Respuesta a las Crisis asistirán a la Autoridad de Seguridad del SEAE en la gestión de los aspectos relacionados con la seguridad de los procesos de continuidad de las actividades del SEAE como parte de la planificación general de la continuidad de las actividades del SEAE.

Artículo 19

Asesoramiento en materia de viajes para las misiones fuera de la UE

La Dirección encargada del Centro de Respuesta a las Crisis velará por la disponibilidad de asesoramiento en materia de viajes para las misiones fuera de la UE del personal bajo la responsabilidad del SEAE, utilizando los recursos de todos sus servicios pertinentes, en particular el INTCEN, la célula de contrainteligencia de la Dirección General de Gestión de Recursos, los departamentos geográficos y las Delegaciones de la Unión.

Previa solicitud, la Dirección encargada del Centro de Respuesta a las Crisis prestará, utilizando los recursos anteriormente indicados, asesoramiento específico en materia de viajes para las misiones del personal bajo la responsabilidad del SEAE en terceros Estados que presenten un nivel de riesgo elevado o incrementado.

Artículo 20

Salud y seguridad

Las normas de seguridad del SEAE completan las normas del SEAE para la protección de la salud y seguridad, tal como han sido adoptadas por el Alto Representante.

Artículo 21

Aplicación y revisión

1. La Autoridad de Seguridad del SEAE, previa consulta al Comité de Seguridad del SEAE, si procede, aprobará directrices de seguridad que establezcan todas las medidas necesarias para la aplicación de dichas normas en el SEAE y creará la capacidad necesaria para cubrir todos los aspectos de la seguridad en estrecha colaboración con las autoridades competentes en este ámbito de los Estados miembros, con el apoyo de los servicios pertinentes de las instituciones de la UE.

2. De conformidad con el artículo 4, apartado 5, de la Decisión 2010/427/UE del Consejo y cuando sea necesario, el SEAE podría celebrar acuerdos entre servicios con los servicios pertinentes de la Secretaría General del Consejo y de la Comisión.

3. El AR garantizará la coherencia general de la aplicación de la presente Decisión y someterá a revisión estas normas de seguridad.

4. Las normas de seguridad del SEAE deberán aplicarse en estrecha colaboración con las autoridades competentes en materia de seguridad de los Estados miembros.

5. El SEAE velará por que se tengan en cuenta todos los aspectos de los procedimientos de seguridad en el sistema de respuesta a crisis del SEAE.

6. El secretario general, como Autoridad de Seguridad, el director de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y el director del Centro de Respuesta a las Crisis velarán por la aplicación de la presente Decisión.

Artículo 22

Sustitución de anteriores decisiones

La presente Decisión deroga y sustituye la Decisión ADMIN (2017)10 de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 19 de septiembre de 2017, sobre las normas de seguridad del Servicio Europeo de Acción Exterior ([5]).

Artículo 23

Disposiciones finales

La presente Decisión entrará en vigor en la fecha de su firma.

Se publicará en el *Diario Oficial de la Unión Europea*.

Las Autoridad de Seguridad del SEAE deberán informar, debida y oportunamente, a todo el personal que entre en el ámbito de aplicación de la presente Decisión y sus anexos, del contenido de esta, de su entrada en vigor y de cualesquiera modificaciones posteriores de esta.

Hecho en Bruselas, el 19 de junio de 2023.

Josep BORRELL FONTELLES
Alto Representante de la Unión
para Asuntos Exteriores y Política de Seguridad

([5]) DO C 126 de 10.4.2018, p. 1.

ANEXO A

PRINCIPIOS Y NORMAS DE PROTECCIÓN DE LA ICUE

Artículo 1

Objeto, ámbito de aplicación y definiciones

1. El presente anexo establece los principios básicos y las normas mínimas de seguridad para la protección de la ICUE.

2. Dichos principios básicos y normas mínimas se aplicarán al SEAE y al personal bajo la responsabilidad del propio SEAE, tal como se menciona y define respectivamente en los artículos 1 y 2 de la presente Decisión.

Artículo 2

Definición de ICUE, clasificaciones de seguridad y marcas

1. Por «información clasificada de la UE» (ICUE) se entenderá toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios de sus Estados miembros.

2. La ICUE se clasificará en uno de los grados siguientes:

a) TRÈS SECRET UE/EU TOP SECRET: información y material cuya revelación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o varios de sus Estados miembros;

b) SECRET UE/EU SECRET: información y material cuya revelación no autorizada pueda causar un perjuicio grave a los intereses esenciales de la Unión Europea o de uno o varios de sus Estados miembros;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: información y material cuya revelación no autorizada pueda causar perjuicio a los intereses esenciales de la Unión Europea o de uno o varios de sus Estados miembros;

d) RESTREINT UE/EU RESTRICTED: información y material cuya revelación no autorizada pueda resultar desfavorable para los intereses de la Unión o de uno o varios de sus Estados miembros.

3. La ICUE llevará una marca de clasificación de seguridad de conformidad con el apartado 2. Podrá llevar marcas suplementarias para designar el ámbito de actividad al que se refiere, identificar el originador, limitar la difusión, restringir su utilización o indicar la medida en que puede ser cedida.

Artículo 3

Gestión de la clasificación

1. EL SEAE se asegurará de que la ICUE se clasifique adecuadamente, quede claramente marcada como información clasificada y solo conserve su grado de clasificación mientras sea necesario.

2. No se podrá rebajar el grado de clasificación de la ICUE ni desclasificarla, ni modificar o suprimir las marcas a que se refiere el artículo 2, apartado 3, sin el consentimiento previo por escrito del originador.

3. La Autoridad de Seguridad del SEAE aprobará, tras consultar al Comité de Seguridad del SEAE con arreglo al artículo 15, apartado 5, de la presente Decisión, directrices de seguridad para la creación de ICUE que incluirá una guía práctica de clasificación.

Artículo 4

Protección de la información clasificada

1. La ICUE se protegerá de conformidad con la presente Decisión.

2. El poseedor de cualquier ICUE tendrá la responsabilidad de protegerla de conformidad con la presente Decisión.

3. Cuando los Estados miembros introduzcan en las estructuras o redes del SEAE información clasificada que lleve una marca nacional de clasificación de seguridad, el SEAE protegerá dicha información con arreglo a los requisitos aplicables a la ICUE del grado equivalente, según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el apéndice B.

El SEAE establecerá procedimientos adecuados para mantener registros precisos de los originadores de:

— la información clasificada recibida por el SEAE; y

— el material fuente incluido en la información clasificada originada por el SEAE.

El Comité de Seguridad del SEAE será informado de estos procedimientos.

4. Grandes cantidades de ICUE o una compilación de esta podrán justificar un grado de protección que corresponda a una clasificación más elevada que la de sus componentes.

Artículo 5

Seguridad en el personal para el manejo de información clasificada de la UE

1. Por «seguridad en el personal» se entenderá la aplicación de medidas que garanticen que el acceso a la ICUE se concede únicamente a personas que:

— tengan necesidad de conocerla;

— hayan sido habilitadas para el grado de clasificación correspondiente para acceder a información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior, o bien hayan sido debidamente autorizadas en virtud de sus funciones con arreglo a las leyes y reglamentos nacionales, y

— hayan sido instruidas sobre sus responsabilidades.

2. Los procedimientos de habilitación personal de seguridad (HPS) determinarán si una persona puede ser autorizada para acceder a la ICUE, teniendo en cuenta su lealtad, honradez y fiabilidad.

3. Antes de poder acceder a ICUE y, posteriormente, a intervalos periódicos, todas las personas deberán ser instruidas sobre sus responsabilidades en materia de protección de la ICUE conforme a lo dispuesto en la presente Decisión y aceptar por escrito dichas responsabilidades.

4. Las disposiciones para la aplicación del presente artículo figuran en el anexo A I.

Artículo 6

Seguridad física de la información clasificada de la UE

1. Por «seguridad física» se entenderá la aplicación de medidas de protección física y técnica para impedir el acceso no autorizado a ICUE.

2. Las medidas de seguridad física estarán concebidas para impedir la entrada, subrepticia o por la fuerza, de intrusos, para disuadir, impedir y descubrir actividades no autorizadas y para permitir la diferenciación del personal en lo que respecta al acceso a ICUE según el principio de necesidad de conocer el contenido de dicha información. Estas medidas se determinarán a partir de un proceso de gestión del riesgo.

3. Se establecerán medidas de seguridad física en todos los locales, edificios, oficinas, salas y demás zonas en que se maneje o almacene ICUE, incluidas las zonas que alberguen sistemas de información y comunicaciones, en el sentido definido en el apéndice A de la presente Decisión.

4. Las zonas en que se almacene ICUE de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior se establecerán como Zonas de Acceso Restringido, de conformidad con el anexo A II, y serán aprobadas por la Autoridad de Seguridad del SEAE.

5. Para la protección de ICUE de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior solo podrán emplearse equipos o dispositivos aprobados.

6. Las disposiciones para la aplicación del presente artículo figuran en el anexo A II.

Artículo 7

Tratamiento de la información clasificada

1. Por «tratamiento de la información clasificada» se entenderá la aplicación de medidas administrativas de control de la ICUE a lo largo de todo su ciclo de vida que completen las medidas contempladas en los artículos 5, 6 y 8 y contribuyan, así, a disuadir, descubrir y subsanar cualquier acto deliberado o accidental que pueda suponer la pérdida o comprometimiento de dicha información. Estas medidas se refieren, en particular, a la producción, registro, copia, traducción, traslado, manejo, almacenamiento y destrucción de ICUE.

2. La información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior se inscribirá en un registro para fines de seguridad antes de ser distribuida y al ser recibida. Las autoridades competentes del SEAE establecerán a tal fin un sistema de registro. La información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» se inscribirá en registros especiales.

3. Los servicios y locales en los que se maneje o almacene ICUE serán inspeccionados periódicamente por la Autoridad de Seguridad del SEAE.

4. La transmisión de la ICUE entre los distintos servicios y locales fuera de las zonas físicamente protegidas se llevará a cabo del siguiente modo:

a) como norma general, la ICUE se transmitirá por medios electrónicos que estén protegidos con productos criptográficos aprobados de conformidad con lo dispuesto en el artículo 7, apartado 5, de la presente Decisión, y de acuerdo con procedimientos operativos de seguridad claramente definidos;

b) en caso de no utilizarse los medios contemplados en la letra a), la ICUE se transportará por cualquiera de los siguientes medios:

   i) medios electrónicos (por ejemplo, llaves USB, discos compactos o discos duros) que estén protegidos con productos criptográficos aprobados de conformidad con lo dispuesto en el artículo 8, apartado 5, de la presente Decisión; o

   ii) en todos los demás casos, según las prescripciones de la Autoridad de Seguridad del SEAE y de acuerdo con las medidas pertinentes de protección establecidas en el anexo A III, sección V.

5. Las disposiciones para la aplicación del presente artículo figuran en el anexo A III.

Artículo 8

Protección de la ICUE manejada en los sistemas de información y comunicaciones

1. Por «garantía de la información» (GI) en el ámbito de los sistemas de información y comunicaciones, se entenderá la confianza en que esos sistemas protejan la información que manejan y funcionen como es necesario que lo hagan, cuando así se precise, bajo el control de sus legítimos usuarios. Una GI efectiva ha de asegurar unos niveles apropiados de confidencialidad, integridad, disponibilidad, no repudio y autenticidad. La GI se basará en un proceso de gestión del riesgo.

2. Los SIC manejarán la ICUE de conformidad con el concepto de GI.

3. Todos los SIC que manejen ICUE serán objeto de un proceso de acreditación. La acreditación tendrá por objeto obtener garantías de que se han aplicado todas las medidas de seguridad oportunas y se ha logrado un grado de protección suficiente de la ICUE y los SIC, de conformidad con la presente Decisión. La declaración de acreditación determinará el grado máximo de clasificación de la información que pueda manejarse en un SIC, así como las condiciones correspondientes.

4. Los SIC que manejen información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior deberán estar protegidos de tal manera que la información no pueda verse comprometida como consecuencia de emanaciones electromagnéticas no intencionadas («medidas de seguridad TEMPEST»).

5. Cuando la protección de la ICUE se efectúe mediante productos criptográficos, esos productos deberán estar aprobados con arreglo al artículo 8, apartado 5, de la presente Decisión.

6. Durante la transmisión de la ICUE mediante medios electrónicos, se emplearán productos criptológicos aprobados. Sin perjuicio de este requisito, se podrán aplicar procedimientos específicos en circunstancias urgentes o en configuraciones técnicas específicas, según se indica en el anexo A IV.

7. Con arreglo al artículo 8, apartado 6, de la presente Decisión, se establecerán, en la medida necesaria, las siguientes funciones de GI:

a) una Autoridad de Garantía de la Información (AGI);

b) una Autoridad TEMPEST;

c) una Autoridad de Certificación Criptológica (ACC);

d) una Autoridad de Distribución Criptológica (ADC).

8. Con arreglo al artículo 8, apartado 7, de la presente Decisión, se establecerá para cada sistema:

a) una Autoridad de Acreditación de Seguridad (AAS);

b) una Autoridad Operativa de Garantía de la Información (AOGI).

9. Las disposiciones para la aplicación del presente artículo figuran en el anexo A IV.

Artículo 9

Seguridad industrial

1. Por «seguridad industrial» se entenderá la aplicación de medidas encaminadas a garantizar la protección de la ICUE por los contratistas o subcontratistas durante las negociaciones precontractuales y durante toda la vigencia de los contratos clasificados. Por norma general, estos contratos no podrán suponer el acceso a información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET».

2. El SEAE podrá encomendar, mediante contrato, a sociedades industriales u otro tipo de entidades registradas en un Estado miembro o en un tercer Estado que haya celebrado un acuerdo de seguridad de la información o un acuerdo administrativo de conformidad con el artículo 10, apartado 1, del anexo A, el desempeño de funciones que conlleven el acceso a ICUE o su manejo o almacenamiento.

3. Cuando actúe como órgano de contratación, el SEAE se asegurará, al adjudicar contratos clasificados a sociedades industriales u otro tipo de entidades, de que se cumplan las normas mínimas sobre seguridad industrial que establece la presente Decisión y se indican en el contrato. Garantizará el cumplimiento de dichas normas mínimas a través de la ANS o la ASD correspondiente.

4. Los contratistas y subcontratistas registrados en un Estado miembro que participen en contratos o subcontratos clasificados que requieran el manejo y almacenamiento de información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET» en sus establecimientos, ya sea en la ejecución de dichos contratos o durante la fase precontractual, deberán poseer una habilitación de seguridad de establecimiento del grado de clasificación requerido, emitida por la ANS, la ASD o cualquier otra autoridad de seguridad competente de dicho Estado miembro.

5. El personal del contratista o subcontratista que deba tener acceso a información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET» para ejecutar un contrato clasificado deberá poseer una habilitación personal de seguridad (HPS) concedida por la ANS, la ASD o cualquier otra autoridad de seguridad competente que corresponda, de conformidad con las disposiciones legales y reglamentarias nacionales y las normas mínimas de seguridad establecidas en el anexo A I.

6. Las disposiciones de aplicación del presente artículo figuran en el anexo A V.

Artículo 10

Intercambio de información clasificada con terceros Estados y organizaciones internacionales

1. El SEAE solo podrá intercambiar ICUE con un tercer Estado o una organización internacional cuando:

a) esté en vigor un acuerdo de seguridad de la información entre la UE y ese tercer Estado u organización internacional, celebrado de conformidad con el artículo 37 del TUE y el artículo 218 del TFUE; o

b) esté en vigor un acuerdo administrativo entre la AR y las autoridades competentes en materia de seguridad de ese tercer Estado u organización internacional para el intercambio de información clasificada, en principio no superior al grado «RESTREINT UE/EU RESTRICTED», celebrado de conformidad con el procedimiento establecido en el artículo 15, apartado 5, de la presente Decisión; o

c) sea aplicable un marco o acuerdo *ad hoc* de participación entre la UE y ese tercer Estado en el contexto de una operación de gestión de crisis de la PCSD, celebrado de conformidad con el artículo 37 del TUE y el artículo 218 del TFUE,

y se cumplan las condiciones establecidas en dicho instrumento.

Las excepciones a la norma general anterior se indican en el anexo A VI, sección V.

2. Los acuerdos administrativos a que se refiere el apartado 1, letra b), contendrán disposiciones que garanticen que los terceros países o las organizaciones internacionales que reciban ICUE protegerán dicha información de manera acorde con su grado de clasificación y conforme a normas mínimas que no sean menos estrictas que las que establece la presente Decisión.

La información intercambiada en virtud de los acuerdos contemplados en el apartado 1, letra c), se limitará a la relativa a las operaciones PCSD en las que participe el tercer Estado de que se trate, sobre la base de dichos acuerdos y con arreglo a lo dispuesto en estos.

3. Si la Unión y el tercer Estado o la organización internacional contribuyente celebran ulteriormente un acuerdo de seguridad de la información, este acuerdo sustituirá a la disposición en materia de intercambio de información clasificada establecida en cualquier acuerdo marco de participación, acuerdo de participación *ad hoc* o acuerdo administrativo *ad hoc* previo en lo que se refiere al intercambio y manejo de ICUE.

4. La ICUE generada a efectos de la operación PCSD podrá ser revelada al personal destinado en comisión de servicio para dicha operación por terceros Estados u organizaciones internacionales de conformidad con lo dispuesto en los puntos 1 a 3 del anexo A VI. Cuando se conceda autorización de acceso a ICUE en los locales o en los SIC de una operación PCSD a dicho personal, se aplicarán las medidas necesarias (incluida la grabación de la ICUE revelada) para evitar riesgos de pérdida o comprometimiento de la información. Estas medidas se determinarán en los documentos de planificación o de misión.

5. Se organizarán visitas de evaluación a terceros Estados y organizaciones internacionales, tal como se indica en el artículo 17 de la presente Decisión, a fin de verificar la eficacia de las medidas de seguridad adoptadas en estos para proteger la ICUE intercambiada.

6. La decisión de ceder ICUE que obre en poder del SEAE a un tercer Estado u organización internacional se adoptará atendiendo a las circunstancias de cada caso, en función de la naturaleza y el contenido de la información, de la necesidad de conocer del destinatario y de la utilidad que pueda tener para la UE.

El SEAE solicitará el consentimiento escrito de cualquier entidad que haya proporcionado información clasificada como material fuente para la ICUE producida por el SEAE para confirmar que no haya objeciones a la cesión.

Si el originador de la información clasificada que se desea ceder no es el SEAE, este último deberá recabar el consentimiento por escrito del originador antes de comunicarla.

Si el SEAE no puede determinar el originador, la Autoridad de Seguridad del SEAE asumirá la responsabilidad de aquel tras obtener el dictamen favorable unánime de los Estados miembros representados en el Comité de Seguridad del SEAE.

7. Las disposiciones para la aplicación del presente artículo figuran en el anexo A VI.

Artículo 11

Fallos en la seguridad y comprometimiento de la información clasificada

1. Todo fallo o sospecha de fallo en la seguridad y todo comprometimiento o sospecha de comprometimiento de la información clasificada deberá notificarse inmediatamente a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, que informará, si procede, al Estado o Estados miembros afectados y a cualquier otra entidad afectada.

2. Cuando se tenga conocimiento o sospechas fundadas de que se ha comprometido o perdido información clasificada, la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE informará a la ANS del Estado o Estados miembros afectados y tomará todas las medidas oportunas, de conformidad con las disposiciones legales y reglamentarias pertinentes, para:

a) proteger las pruebas;

b) velar por que el personal que investigue el caso con el fin de esclarecer los hechos no esté directamente implicado en el fallo o comprometimiento;

c) informar inmediatamente al originador y a cualquier otra entidad afectada;

d) tomar medidas adecuadas a fin de impedir que se repitan esos hechos;

e) evaluar el posible perjuicio causado a los intereses de la UE o de los Estados miembros; y

f) notificar a las autoridades pertinentes los efectos del comprometimiento real o sospecha de comprometimiento y las medidas adoptadas.

3. Cualquier miembro del personal bajo la responsabilidad del SEAE que sea responsable de un fallo en la seguridad por incumplimiento de las normas de seguridad establecidas en la presente Decisión podrá ser objeto de medidas disciplinarias de conformidad con la normativa aplicable.

Todo individuo que sea responsable del comprometimiento o pérdida de información clasificada estará sujeto a medidas disciplinarias o legales de conformidad con las disposiciones legales, normativas y reglamentarias aplicables.

4. Mientras esté en curso una investigación sobre un fallo en la seguridad o un comprometimiento de la información, el jefe de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE podrá suspender el acceso de personas a la ICUE y a las dependencias del SEAE. Se informará de inmediato de esta decisión a la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión, a la Oficina de Seguridad de la Secretaría General del Consejo o a la ANS del Estado o Estados miembros afectados y a cualquier otra entidad afectada.

ANEXO A I

SEGURIDAD EN EL PERSONAL

I. INTRODUCCIÓN

1. El presente anexo establece las disposiciones de aplicación del artículo 5 del anexo A. En concreto, define los criterios que debe aplicar el SEAE para determinar si una persona, teniendo en cuenta su lealtad, honradez y fiabilidad, puede ser autorizada para acceder a ICUE, y los procedimientos administrativos y de investigación que han de seguirse a tal efecto.

2. Por «habilitación personal de seguridad» (HPS) para acceder a ICUE se entenderá la declaración de una autoridad competente de un Estado miembro, efectuada al término de una investigación de seguridad realizada por las autoridades competentes del Estado miembro, mediante la cual se acredita que una persona puede tener acceso a ICUE de un determinado grado («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información; de la persona que se ajuste a esta descripción se dirá que está «habilitada».

3. Por «certificado de habilitación personal de seguridad» (CHPS) se entenderá un certificado expedido por la Autoridad de Seguridad del SEAE que acredite que una persona está habilitada e indique el grado de ICUE al que puede tener acceso, el período de validez de la HPS correspondiente y la fecha de caducidad del propio certificado.

4. Por «autorización para acceder a ICUE» se entenderá una autorización de la Autoridad de Seguridad del SEAE concedida de conformidad con la presente Decisión previa emisión de una HPS por las autoridades competentes de un Estado miembro y que acredite que una persona puede tener acceso a ICUE de un determinado grado («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información; de la persona que se ajuste a esta descripción se dirá que está «habilitada».

II. AUTORIZACIÓN DE ACCESO A LA ICUE

5. El acceso a la información clasificada de grado «RESTREINT UE/EU RESTRICTED» no requerirá habilitación de seguridad y se concederá:

   a) una vez establecido el vínculo estatutario o contractual de la persona con el SEAE;

   b) una vez determinada la necesidad de la persona de conocer;

   c) una vez la persona haya sido instruida sobre las normas y procedimientos de seguridad para la protección de la ICUE y haya aceptado por escrito sus responsabilidades en lo que respecta a la protección de la ICUE de conformidad con la presente Decisión.

6. Solo se concederá autorización para acceder a información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior a una persona:

   a) una vez establecido el vínculo estatutario o contractual de la persona con el SEAE;

   b) cuya necesidad de conocer se haya determinado;

   c) a quien se haya concedido una HPS de grado correspondiente, o a quien se haya autorizado debidamente en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales; y

   d) que haya sido instruida sobre las normas y procedimientos de seguridad para la protección de la ICUE y haya aceptado por escrito sus responsabilidades en lo que respecta a la protección de dicha información.

7. El SEAE indicará los puestos de sus estructuras que requieran acceso a información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior y, por tanto, necesiten una HPS del grado correspondiente, como se indica en el punto 4 anterior.

8. El personal del SEAE deberá declarar si posee la nacionalidad de más de un país.

Procedimientos de solicitud de HPS en el SEAE

9. Para el personal del SEAE, la Autoridad de Seguridad del SEAE remitirá el cuestionario personal de seguridad, una vez cumplimentado, a la ANS del Estado miembro del que sea nacional la persona, para solicitar la realización de la investigación de seguridad correspondiente al grado de ICUE para el que se requiera el acceso.

10. Cuando una persona posea la nacionalidad de más de un país, la solicitud de investigación deberá enviarse a la ANS del país con cuya nacionalidad se haya contratado a dicha persona.

11. Cuando llegue a conocimiento del SEAE información pertinente para la investigación de seguridad sobre una persona que ha solicitado una HPS, el SEAE, actuando de acuerdo con las disposiciones legales y reglamentarias pertinentes, la notificará a la ANS pertinente.

12. Una vez concluida la investigación de seguridad, la ANS comunicará los resultados a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE.

    a) Si los resultados de la investigación de seguridad permiten garantizar que no se conoce ningún dato desfavorable que ponga en entredicho la lealtad, honradez y fiabilidad de la persona, la Autoridad de Seguridad del SEAE podrá otorgarle una autorización para acceder a ICUE del grado pertinente hasta una fecha determinada.

    b) El SEAE deberá adoptar todas las medidas pertinentes para garantizar la correcta aplicación de las condiciones o restricciones impuestas por la ANS. Se informará a la ANS del resultado.

    c) Si los resultados de la investigación de seguridad no aseguran dicha garantía, la Autoridad de Seguridad del SEAE lo notificará a la persona afectada, que podrá requerir ser oído por esta. La Autoridad de Seguridad del SEAE podrá pedir a la ANS competente cuantas aclaraciones le pueda facilitar, de conformidad con sus disposiciones legales y reglamentarias. De confirmarse el resultado anterior, no se concederá la autorización para acceder a ICUE. En tal caso, el SEAE adoptará las medidas pertinentes para garantizar que se deniegue al solicitante todo acceso a ICUE.

13. La investigación de seguridad, junto con los resultados obtenidos, en los que la Autoridad de Seguridad del SEAE basará su decisión de conceder o no una autorización para acceder a ICUE, deberá ser conforme a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión, incluido todo lo relativo a recursos. Se podrán recurrir las decisiones de la Autoridad de Seguridad del SEAE en las condiciones establecidas en los artículos 90 y 91 del Estatuto de los funcionarios.

14. La garantía en la que se base una HPS, siempre que siga siendo válida, lo será para cualquier nombramiento de la persona en el SEAE, en la Secretaría General del Consejo o en la Comisión.

15. El SEAE aceptará la autorización para acceder a ICUE concedida por otra institución, órgano u organismo de la Unión, siempre que siga siendo válida. La autorización valdrá para cualquier nombramiento de la persona en el SEAE. La institución, órgano u organismo de la Unión que contrate a la persona notificará a la ANS correspondiente el cambio de empleador.

16. En caso de que el período de servicio de la persona no haya comenzado al término de 12 meses a partir de la notificación del resultado de la investigación de seguridad a la Autoridad de Seguridad del SEAE, o en caso de que haya una interrupción de 12 meses en el tiempo de servicio de esa misma persona durante el cual no haya estado empleada en el SEAE, en otras instituciones, órganos u organismos de la UE, o en un puesto de la Administración pública de un Estado miembro que requiera acceso a información clasificada, el resultado de la investigación se remitirá de nuevo a la ANS correspondiente para que confirme que sigue siendo válido y adecuado.

17. Si el SEAE tuviera conocimiento de que una persona que disponga de una HPS válida representa un riesgo para la seguridad, el SEAE, actuando conforme a las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS correspondiente y podrá suspender dicho acceso a ICUE o retirar la autorización para acceder a ICUE. Si una ANS notifica al SEAE la retirada de una garantía concedida de conformidad con el apartado 12, letra a), al titular de una autorización válida para acceder a ICUE, la Autoridad de Seguridad del SEAE podrá pedir a la ANS cuantas aclaraciones pueda facilitar, de conformidad con sus disposiciones legales y reglamentarias nacionales. Si se confirma la información desfavorable, se le retirará la autorización anteriormente indicada y se le excluirá del acceso a la ICUE y de los puestos en los que pudiera tener acceso a dicha información o poner en peligro la seguridad.

18. La decisión de retirar una autorización para acceder a ICUE a un miembro del personal del SEAE y, en su caso, los motivos para hacerlo se comunicarán a la persona, que podrá requerir ser oída por la Autoridad de Seguridad del SEAE. La información facilitada por la ANS deberá ajustarse a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión, incluidas las relativas a los recursos. Se podrán recurrir las decisiones de la Autoridad de Seguridad del SEAE en las condiciones establecidas en los artículos 90 y 91 del Estatuto de los funcionarios.

19. Los expertos nacionales destinados en el SEAE en comisión de servicio para un puesto que requiera acceso a información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior deberán presentar a la Autoridad de Seguridad del SEAE una HPS válida para acceder a ICUE antes de asumir sus funciones. El procedimiento anterior será gestionado por el Estado miembro de procedencia.

Registros de las HPS

20. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE deberá mantener una base de datos sobre la situación en materia de habilitación de seguridad de todo el personal bajo su responsabilidad y del personal de sus contratistas. Estos registros indicarán el grado de la ICUE al que la persona puede tener acceso («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior), la fecha de concesión de la habilitación y su período de validez.

21. Se deberán establecer procedimientos adecuados de coordinación con los Estados miembros y otras instituciones, órganos y organismos de la UE para garantizar que el SEAE mantenga un registro global y exacto de la situación en materia de habilitación de seguridad de todo el personal bajo su responsabilidad y del personal de sus contratistas.

22. La Autoridad de Seguridad del SEAE podrá expedir un Certificado de Habilitación Personal de Seguridad (CHPS) que acredite el grado de ICUE al que puede tener acceso la persona («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior), el período de validez de la autorización o HPS correspondiente y la fecha de caducidad del propio certificado.

Excepciones al requisito de titularidad de una HPS

23. Las personas debidamente autorizadas para acceder a ICUE en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales, serán informadas, cuando proceda, de sus obligaciones en materia de protección de la ICUE por la Dirección encargada de la seguridad de la sede y la seguridad de la información en el SEAE.

III. FORMACIÓN Y CONCIENCIACIÓN EN CUESTIONES DE SEGURIDAD

24. Antes de recibir la autorización de acceso a la ICUE, todas las personas reconocerán en una declaración escrita que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias del comprometimiento de esta información. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE llevará un registro de estas declaraciones escritas.

25. Desde un principio se concienciará a todas las personas que estén autorizadas para acceder a ICUE o que deban manejar este tipo de información respecto de las amenazas a la seguridad, sobre las que se les instruirá periódicamente. Dichas personas deberán dar cuenta inmediatamente a los coordinadores de seguridad de los departamentos o Delegaciones correspondientes y a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE de cualquier actitud o actividad que consideren sospechosa o inusual.

26. Todas las personas a las que se haya concedido acceso a ICUE estarán sujetas a medidas de seguridad continua en el personal (por ejemplo, seguimiento) durante el tiempo en que manejen ICUE. La seguridad continua en el personal será responsabilidad de:

    a) las personas a las que se haya concedido acceso a ICUE, que serán personalmente responsables de su propio comportamiento de seguridad y deberán comunicar de inmediato a las autoridades de seguridad correspondientes cualquier actitud o actividad que consideren sospechosa o inusual, y cualesquiera cambios en sus circunstancias personales que puedan incidir en su HPS o autorización para acceder a ICUE;

b) los superiores jerárquicos, que serán responsables de determinar la necesidad de conocer de cada persona y de garantizar que su personal es consciente de las medidas de seguridad y de su responsabilidad de proteger la ICUE, de supervisar el comportamiento de seguridad de su personal y de resolver problemas de seguridad por sí mismos o informar a las autoridades de seguridad correspondientes de cualquier información desfavorable que pueda incidir en las HPS o las autorizaciones para acceder a ICUE de su personal;

c) los agentes de la organización de seguridad del SEAE, tal como se indican en el artículo 12 de la presente Decisión, que serán responsables de organizar sesiones informativas en cuestiones de seguridad para garantizar que el personal de su zona sea periódicamente informado, de fomentar una sólida cultura de seguridad en su ámbito de responsabilidad, de implantar medidas para supervisar el comportamiento de seguridad del personal y de informar a las autoridades de seguridad pertinentes de cualquier información desfavorable que pueda incidir en la HPS de cualquier persona;

d) el SEAE y los Estados miembros, que deberán establecer los canales necesarios para comunicar información que pueda incidir en la HPS o la autorización de para acceder a ICUE de una persona.

27. Todas las personas que dejen de desempeñar funciones que requieran el acceso a ICUE serán instruidas sobre su obligación de seguir protegiendo dicha información y, en su caso, deberán reconocer tal obligación por escrito.

IV. CIRCUNSTANCIAS EXCEPCIONALES

28. Por razones de urgencia, cuando esté debidamente justificado en interés del SEAE y en espera de la conclusión de una investigación de seguridad completa, la Autoridad de Seguridad del SEAE podrá conceder a funcionarios y otros agentes del SEAE una autorización temporal para acceder a ICUE para una función específica, tras haber consultado a la ANS del Estado miembro del que sea nacional la persona y con supeditación al resultado de las indagaciones preliminares encaminadas a verificar que no se conoce ninguna información desfavorable de esta. Las investigaciones de seguridad completa deberán concluirse lo antes posible. La validez de estas autorizaciones temporales no será superior a seis meses ni permitirá acceder a información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET». Todas las personas a las que se haya otorgado autorización temporal reconocerán en una declaración escrita que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias del comprometimiento de esta información. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE llevará un registro de estas declaraciones escritas.

29. En caso de que se vaya a destinar a una persona a un puesto que requiera una HPS de un grado superior al que posea en ese momento, el nombramiento podrá efectuarse a título provisional, siempre que:

a) el correspondiente superior jerárquico de la persona, a nivel de director, director general o jefe de delegación, según corresponda, justifique por escrito la necesidad imperiosa de acceso a información clasificada de la UE de un grado superior;

b) el acceso se limite a elementos concretos de información clasificada de la UE para el desempeño de su función;

c) la persona posea una HPS válida;

d) se hayan iniciado los trámites para la obtención de la autorización de acceso del nivel que el puesto requiera;

e) la autoridad competente haya comprobado a su satisfacción que la persona no ha infringido de manera grave o reiterada las normas de seguridad;

f) el nombramiento de la persona haya sido aprobado por la autoridad competente del SEAE;

g) se haya consultado a la ANS/ASD que haya emitido la HPS de la persona y no se hayan recibido objeciones; y

h) el encargado del registro o registro secundario haga constar la excepción, con una descripción de la información para la cual se haya autorizado el acceso.

30. Este procedimiento se utilizará para un único acceso a ICUE del grado inmediatamente superior a aquel para el que la persona esté habilitada. No podrá utilizarse este procedimiento de forma reiterada.

31. En circunstancias muy excepcionales, como misiones en un medio hostil o durante períodos de incremento de la tensión internacional en los que así lo requieran medidas de urgencia, y en particular cuando estén en peligro vidas humanas, el AR, la Autoridad de Seguridad del SEAE o el director general de Gestión de Recursos podrán autorizar, a ser posible por escrito, el acceso a información de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET» a personas que no posean la HPS exigida, siempre que dicha autorización sea imprescindible. La Dirección encargada de la seguridad y la seguridad de la información del SEAE registrará dicha autorización junto con una descripción de la información para la cual se haya autorizado el acceso.

32. En el caso de la información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET», este acceso de urgencia estará limitado a los nacionales de la UE que hayan sido autorizados para acceder o bien a información clasificada de grado nacional equivalente a «TRÈS SECRET UE/EU TOP SECRET» o bien a información clasificada de grado «SECRET UE/EU SECRET».

33. El Comité de Seguridad del SEAE será informado de los casos en los que se recurra al procedimiento establecido en los apartados 31 y 32.

34. El Comité de Seguridad del SEAE recibirá un informe anual sobre la utilización de los procedimientos establecidos en la presente sección.

V. ASISTENCIA A REUNIONES EN LA SEDE DEL SEAE Y EN LAS DELEGACIONES DE LA UNIÓN

35. Las personas designadas para participar en reuniones en la sede del SEAE y en las Delegaciones de la Unión en las que se vaya a debatir información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior solo podrán hacerlo previa confirmación de su situación en materia de HPS. Por lo que respecta a los representantes de los Estados miembros y funcionarios de la Secretaría General del Consejo y de la Comisión, las autoridades pertinentes deberán remitir previamente un CHPS u otra prueba de HPS a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE o al coordinador de seguridad de la Delegación de la Unión; en casos excepcionales, dicha prueba podrá ser presentada por la persona afectada. Cuando proceda, podrá utilizarse una lista recapitulativa de nombres en la que figuren las pruebas pertinentes de su HPS.

36. Cuando se retire una HPS que permita acceder a ICUE a una persona cuyas funciones requieran la asistencia a reuniones en la sede del SEAE o en Delegaciones de la Unión en las que vaya a debatirse información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL», la autoridad competente informará de ello a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE.

VI. ACCESO POTENCIAL A ICUE

37. Las personas que en el desempeño de sus funciones tengan probabilidad de acceder a información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior deberán estar debidamente habilitadas o ir escoltadas en todo momento.

38. Los correos, agentes de seguridad y escoltas serán debidamente habilitados para el grado correspondiente o investigados de forma apropiada según las disposiciones legales y reglamentarias nacionales, y se les instruirá de forma periódica sobre los procedimientos de seguridad para la protección de la ICUE y acerca de sus obligaciones en materia de protección de la información que se les confíe o a la que tengan acceso involuntariamente.

ANEXO A II

SEGURIDAD FÍSICA DE LA INFORMACIÓN CLASIFICADA DE LA UE

I. INTRODUCCIÓN

1. El presente anexo establece las disposiciones de aplicación del artículo 6 del anexo A. Define los requisitos mínimos para la protección física de los locales, edificios, oficinas, salas y demás zonas donde se maneje y almacene ICUE, incluidas las zonas que alberguen sistemas de información y comunicaciones.

2. Las medidas de seguridad física estarán concebidas para impedir el acceso no autorizado a ICUE para:

   a) garantizar que la ICUE se maneje y se almacene adecuadamente;

   b) permitir la separación del personal en su acceso a ICUE en función de su necesidad de conocer y, en su caso, de su habilitación de seguridad;

   c) disuadir, impedir y detectar actividades no autorizadas; y

   d) impedir o retrasar la entrada subrepticia o por la fuerza de intrusos.

II REQUISITOS Y MEDIDAS DE SEGURIDAD FÍSICA

3. El SEAE aplicará un proceso de gestión de riesgos para proteger la ICUE en sus respectivos locales, de modo que se garantice un grado de protección física acorde con el riesgo evaluado. El proceso de gestión del riesgo tendrá en cuenta todos los factores pertinentes, en particular:

   a) el grado de clasificación de la ICUE;

   b) la forma y volumen de la ICUE, teniendo presente que grandes cantidades de ICUE o su recopilación podrían requerir la aplicación de medidas de protección más estrictas;

   c) el entorno y la estructura de los edificios o zonas donde se guarde ICUE;

   d) la evaluación de la amenaza de terceros países elaborada por el INTCEN, la célula de contrainteligencia de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y sobre la base, en particular, de los informes de las Delegaciones de la Unión, y

   e) la evaluación de las amenazas que representan tanto los servicios de inteligencia que tienen como objetivo la UE y sus Estados miembros como el sabotaje, el terrorismo, la subversión u otras actividades delictivas.

4. Al aplicar el concepto de defensa en profundidad, la Autoridad de Seguridad del SEAE determinará la combinación apropiada de las siguientes medidas de seguridad física que debe aplicarse. Estas pueden incluir una o más de las siguientes:

   a) barreras perimetrales: se trata de barreras físicas que protegen los límites exteriores de la zona que precisa protección;

   b) sistemas de detección de intrusiones (SDI): estos sistemas pueden emplearse para aumentar el grado de seguridad que brinda la barrera perimetral o, en determinadas salas y edificios, en sustitución o como complemento del personal de seguridad;

   c) controles de acceso: los controles de acceso pueden aplicarse en una instalación, en un edificio o edificios de una instalación o en zonas o salas situadas dentro de un edificio; el control puede realizarse por medios electrónicos o electromecánicos, por medio de personal de seguridad, de un recepcionista o de ambos, o por cualquier otro medio físico;

   d) personal de seguridad: puede emplearse, entre otros recursos, personal de seguridad formado, inspeccionado y, en caso necesario, con la debida habilitación de seguridad para disuadir a posibles intrusos que planeen una entrada encubierta;

   e) sistemas de circuito cerrado de televisión (CCTV): estos sistemas pueden ser utilizados por el personal de seguridad para verificar incidentes y alarmas del SDI en emplazamientos de gran extensión o en el perímetro de una zona;

   f) iluminación de seguridad: la iluminación de seguridad puede emplearse para disuadir a posibles intrusos, además de proporcionar la iluminación necesaria para una vigilancia eficaz, bien directamente por parte del personal de seguridad, bien de forma indirecta a través de un CCTV, y

   g) cualquier otra medida apropiada de seguridad física destinada a disuadir o detectar entradas no autorizadas o a prevenir la pérdida o deterioro de ICUE.

5. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE podrá llevar a cabo, en las entradas y las salidas, registros que disuadan de todo intento no autorizado de introducir material en los locales o edificios o de sacar de ellos ICUE.

6. Cuando exista el riesgo de que una ICUE sea objeto de miradas indiscretas, incluso accidentalmente, se tomarán medidas adecuadas para contrarrestar ese riesgo.

7. Para los nuevos establecimientos, los requisitos de seguridad física y sus especificaciones funcionales se definirán en el momento de la planificación y el diseño de estos. Para los establecimientos ya existentes, los requisitos de seguridad física se aplicarán en la mayor medida posible.

III EQUIPO PARA LA PROTECCIÓN FÍSICA DE LA ICUE

8. La Autoridad de Seguridad del SEAE se asegurará de que el equipo que se adquiera para la protección física de la ICUE (armarios de seguridad, trituradoras de papel, cerraduras, CCTV, sistemas electrónicos de control de acceso, SDI, sistemas de alarma, etc.) cumpla las normas técnicas y los requisitos mínimos aprobados.

9. Las especificaciones técnicas del equipo que vaya a emplearse para la protección física de la ICUE se establecerán en directrices de seguridad que deberán ser aprobadas por el Comité de Seguridad del SEAE.

10. Los sistemas de seguridad se inspeccionarán periódicamente, y se realizará un mantenimiento del equipo con regularidad. Para las operaciones de mantenimiento se tendrá en cuenta el resultado de las inspecciones, a fin de garantizar que el equipo siga funcionando óptimamente.

11. La eficacia de cada medida de seguridad y del sistema de seguridad en su conjunto se reevaluará en cada inspección.

IV. ZONAS FÍSICAMENTE PROTEGIDAS

12. Para la protección física de la ICUE se establecerán dos tipos de zonas físicamente protegidas, o sus equivalentes nacionales:

    a) zonas administrativas, y

    b) zonas de acceso restringido (incluidas las zonas de acceso restringido protegidas por medios técnicos).

13. La Autoridad de Seguridad del SEAE decidirá si una zona cumple los requisitos para ser designada zona administrativa, zona de acceso restringido o zona acceso restringido protegida por medios técnicos.

14. Para las zonas administrativas:

    a) se establecerá un perímetro visiblemente definido que permita el control de personas y, cuando sea posible, de vehículos;

    b) solo se permitirá el acceso a la sede sin acompañamiento a las personas debidamente autorizadas por la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, y en el caso de las Delegaciones de la Unión, por el jefe de la Delegación; y

    c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.

15. Para las zonas de acceso restringido:

    a) se establecerá un perímetro visiblemente definido y protegido en el que se controlen todas las entradas y salidas mediante un sistema de pases o de identificación personal;

    b) solo se permitirá el acceso sin acompañamiento a las personas que tengan una habilitación de seguridad del grado correspondiente y una autorización específica para entrar en la zona por su necesidad de conocer, y

    c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.

16. Cuando la entrada en una zona de acceso restringido equivalga en la práctica a tener acceso directo a la información clasificada que se encuentre en la zona, se aplicarán además los siguientes requisitos:

    a) se indicará con claridad el máximo grado de clasificación de seguridad de la información que se encuentre normalmente en dicha zona;

    b) todos los visitantes necesitarán una autorización específica para acceder a la zona, serán acompañados en todo momento y estarán debidamente habilitados, salvo que se tomen medidas para que no sea posible que accedan a la ICUE, y

    c) los dispositivos electrónicos deberán dejarse fuera de la zona.

17. Las zonas de acceso restringido protegidas contra escuchas serán designadas como zonas de acceso restringido protegidas por medios técnicos. Se aplicarán los requisitos adicionales siguientes:

    a) estas zonas estarán equipadas con sistemas de detección de intrusos, se cerrarán con llave cuando no estén ocupadas y se vigilarán cuando estén ocupadas; todas las llaves se controlarán de acuerdo con lo dispuesto en la sección VI del presente anexo;

    b) todas las personas y el material que entren en estas zonas serán objeto de control;

    c) dichas zonas serán inspeccionadas periódicamente, física o técnicamente, según lo requiera la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE. Además, serán inspeccionadas también siempre que se haya producido o se sospeche que se ha producido una entrada no autorizada; y

    d) no habrá en estas zonas ninguna línea de comunicaciones, teléfono ni otro equipo de comunicaciones, ni aparatos eléctricos o electrónicos, salvo los que estén autorizados.

18. No obstante lo dispuesto en el apartado 17, letra d), antes de ser utilizados en zonas en las que se celebren reuniones o se realicen trabajos relacionados con información clasificada de grado «SECRET UE/EU SECRET» y superior, y en las que la amenaza para la ICUE se considere elevada, todos los dispositivos de comunicación y equipos eléctricos o electrónicos serán examinados en primer lugar por el equipo de contramedidas técnicas de seguridad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, con el fin de garantizar que ninguna información inteligible pueda transmitirse de manera involuntaria o ilícita a través de dichos equipos más allá del perímetro de la zona de acceso restringido de que se trate.

19. Las zonas de acceso restringido que no estén ocupadas por personal de servicio las 24 horas del día se inspeccionarán, en su caso, al final de la jornada normal de trabajo y a intervalos aleatorios fuera de dicha jornada, a menos que se haya instalado en ellas un sistema de detección de intrusos.

20. Se podrán establecer con carácter temporal zonas de acceso restringido y zonas de acceso restringido protegidas por medios técnicos en una zona administrativa para la celebración de una reunión clasificada u otro motivo similar.

21. Para cada zona de acceso restringido se definirán procedimientos operativos de seguridad en los que se disponga lo siguiente:

    a) el grado de la ICUE que puede manejarse o almacenarse en la zona;

    b) las medidas de vigilancia y protección que hayan de aplicarse;

    c) las personas autorizadas para entrar en ella sin acompañamiento en virtud de su necesidad de conocer y de su habilitación de seguridad;

    d) si ha lugar, los procedimientos aplicables a los acompañantes o a la protección de la ICUE cuando se autorice la entrada de cualquier otra persona en la zona; y

    e) cualquier otra medida o procedimiento pertinente.

22. Las cámaras acorazadas, cuando sean necesarias, se ubicarán en zonas de acceso restringido. Los muros, suelos, techos, ventanas y puertas que puedan cerrarse con llave deberán haber sido aprobados por la Autoridad de Seguridad del SEAE y ofrecer una protección equivalente a la de un contenedor de seguridad aprobado para el almacenamiento de ICUE del mismo grado de clasificación.

V. MEDIDAS DE PROTECCIÓN FÍSICA PARA EL MANEJO Y ALMACENAMIENTO DE LA ICUE

23. La ICUE de grado «RESTREINT UE/EU RESTRICTED» se podrá manejar:

a) en una zona de acceso restringido;

b) en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas, o

c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la ICUE de conformidad con los apartados 30 a 42 del anexo A III y se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la Autoridad de Seguridad del SEAE para garantizar que la ICUE esté protegida frente al acceso de personas no autorizadas.

24. La ICUE de grado «RESTREINT UE/EU RESTRICTED» se guardará en muebles de oficina adecuadamente cerrados con llave en las zonas administrativas o las zonas de acceso restringido. La ICUE de dicho grado podrá almacenarse temporalmente fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la Autoridad de Seguridad del SEAE.

25. La ICUE de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o SECRET UE/EU SECRET» se podrá manejar:

a) en una zona de acceso restringido;

b) en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas; o

c) fuera de una zona de acceso restringido o de una zona administrativa siempre que el poseedor:

i) transporte la ICUE de conformidad con los puntos 30 a 42 del anexo III,

ii) se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la Autoridad de Seguridad del SEAE para garantizar que el acceso a la ICUE se impida a personas no autorizadas;

iii) mantenga la ICUE en todo momento bajo su control personal; y

iv) en el caso de documentos en papel, haya notificado el hecho al registro correspondiente.

26. La ICUE de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y «SECRET UE/EU SECRET» se almacenará en una zona de acceso restringido dentro de un contenedor de seguridad o una cámara acorazada.

27. La ICUE de grado «TRÈS SECRET UE/EU TOP SECRET» se manejará en una zona de acceso restringido.

28. 28. La ICUE de grado «TRÈS SECRET UE/EU TOP SECRET» se almacenará en una zona de acceso restringido de la sede en una de las condiciones siguientes:

a) en un contenedor de seguridad conforme a lo dispuesto en el apartado 8, con uno o varios de los controles adicionales siguientes:

i) protección continua o verificación periódica por personal de seguridad o de servicio habilitado,

ii) un SDI aprobado, junto con personal de seguridad para intervención en caso de incidente;

o

b) en una cámara acorazada con SDI, junto con personal de seguridad para intervención en caso de incidente.

29. En el anexo A III se recogen las normas para el transporte de ICUE fuera de las zonas protegidas físicamente.

VI. CONTROL DE LLAVES Y COMBINACIONES EMPLEADAS PARA LA PROTECCIÓN DE ICUE

30. La Autoridad de Seguridad del SEAE definirá procedimientos de gestión de las llaves y las combinaciones de las oficinas, salas, cámaras acorazadas y contenedores de seguridad de todos los locales del SEAE. Estos procedimientos deberán evitar accesos no autorizados.

31. Las combinaciones serán confiadas al menor número posible de personas que necesiten conocerlas. Las combinaciones de los contenedores de seguridad y cámaras acorazadas en los que se guarde ICUE se modificarán:

    a) al recibir un nuevo contenedor;

    b) cada vez que cambie el personal que conoce la combinación;

    c) cada vez que se haya producido o se sospeche que se ha producido una situación de comprometimiento;

    d) cuando se realicen operaciones de mantenimiento o de reparación de una cerradura; y

    e) al menos cada 12 meses.

ANEXO A III

TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA

I. INTRODUCCIÓN

1. El presente anexo contiene las disposiciones de aplicación del artículo 7 del anexo A. Establece las medidas administrativas para controlar la ICUE a lo largo de su ciclo de vida con el fin de prevenir, detectar y subsanar el comprometimiento o la pérdida, accidentales o deliberados, de dicha información.

II GESTIÓN DE LA CLASIFICACIÓN

Clasificaciones y marcas

2. La información se clasificará cuando requiera protección respecto de su confidencialidad.

3. El originador de la ICUE se encargará de determinar el grado de clasificación de seguridad, aplicar el marcado de clasificación de seguridad adecuado, determinar la difusión de la información a los destinatarios previstos y aplicar la marca de posibilidad de cesión, de conformidad con las directrices pertinentes del SEAE sobre la creación y el tratamiento de ICUE.

4. El grado de clasificación de la ICUE se determinará de conformidad con el artículo 2, apartado 2, del anexo A y con referencia a las directrices de seguridad [...] aprobadas de conformidad con el artículo 3, apartado 3, de dicho anexo.

5. La información clasificada de los Estados miembros intercambiada con el SEAE deberá recibir el mismo grado de protección que la ICUE de clasificación equivalente. En el apéndice B de la presente Decisión se puede consultar un cuadro de equivalencias.

6. La clasificación de seguridad y, en su caso, la fecha o acontecimiento concreto a partir de los cuales podrá reducirse el grado de clasificación o desclasificarse se indicarán clara y correctamente, independientemente de que la ICUE sea verbal o figure en soporte de papel, electrónico o de cualquier otro tipo.

7. Las distintas partes (es decir, páginas, apartados, secciones, anexos, apéndices o documentos adjuntos) de un documento determinado podrán requerir una clasificación diferente, lo cual deberá indicarse en consecuencia, incluso cuando se almacenen en forma electrónica.

8. En la medida de lo posible, los documentos que contengan partes con distintos grados de clasificación se estructurarán de tal modo que las partes con un grado de clasificación diferente puedan ser fácilmente reconocidas y separadas, si fuera necesario.

9. El grado global de clasificación de un documento o archivo deberá ser al menos tan alto como el de su componente con mayor grado de clasificación. Cuando se recopile información procedente de diversas fuentes, se revisará el producto final para determinar su grado global de clasificación de seguridad, dado que podría estar justificado un grado de clasificación mayor que el de los componentes que lo forman.

10. La clasificación de una carta o nota de transmisión de documentos será equivalente al grado más elevado de clasificación de los documentos adjuntos. El originador deberá indicar claramente en qué grado está clasificada la información una vez separada de sus documentos adjuntos mediante la marca correspondiente, según el siguiente ejemplo:

CONFIDENTIEL UE/EU CONFIDENTIAL Sin anexos: RESTREINT UE/EU RESTRICTED

Marcas

11. Junto con una de las marcas de la clasificación de seguridad fijadas en el artículo 2, apartado 2, del anexo A, la ICUE podrá llevar marcas adicionales tales como:

    a) un identificador para designar al originador;

    b) cualquier advertencia, código o acrónimo que especifique el ámbito de actividad a que se refiere el documento, así como indicaciones relativas a su distribución específica, basada en el principio de la necesidad de conocer, o a restricciones de su uso; y

    c) marcados de comunicabilidad.

12. Cuando se adopte la decisión de ceder ICUE a un tercer Estado u organización internacional, la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE enviará la información clasificada de que se trate, que deberá llevar una marca de posibilidad de cesión que indique el tercer Estado u organización internacional al que debe cederse.

13. La Autoridad de Seguridad del SEAE adoptará una lista de marcas autorizadas.

Marcas abreviadas de clasificación

14. Podrán utilizarse marcas abreviadas normalizadas de clasificación para indicar el grado de clasificación de los diferentes apartados de un texto. Las marcas de clasificación completas no se sustituirán por abreviaturas.

15. Podrán utilizarse dentro de documentos clasificados de la UE las siguientes abreviaturas normalizadas para indicar el grado de clasificación de secciones o bloques del texto de extensión inferior a una página:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/UE CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Producción de ICUE

16. Cuando se genere un documento clasificado de la UE:

    a) cada página llevará claramente marcado el grado de clasificación;

    b) cada página irá numerada;

    c) el documento deberá llevar un número de referencia y un asunto, que no constituirá en sí mismo información clasificada, salvo que se marque como tal;

    d) el documento estará fechado;

    e) los documentos con clasificación «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior llevarán un número de ejemplar en cada página cuando hayan de distribuirse en varios ejemplares.

17. Cuando no sea posible aplicar el apartado 16 a una ICUE, se tomarán otras medidas adecuadas de conformidad con las directrices de seguridad [...] establecidas con arreglo a la presente Decisión.

Reducción del grado de clasificación y desclasificación de la ICUE

18. En el momento de producir la información, el originador indicará, cuando sea posible, y en especial si se trata de información clasificada de grado «RESTREINT UE/EU RESTRICTED», si el grado de clasificación de la ICUE puede ser reducido o desclasificado a partir de una determinada fecha o tras un acontecimiento concreto.

19. El SEAE revisará periódicamente la ICUE para verificar si el grado de clasificación asignado sigue siendo aplicable. El SEAE creará un sistema para revisar, con una frecuencia mínima quinquenal, el grado de clasificación de la ICUE registrada que haya generado. Dicha revisión no será necesaria cuando el originador haya indicado desde el principio una fecha concreta en la que el grado de clasificación de la información podrá ser automáticamente reducido o en la que la información podrá desclasificarse, y la información haya sido marcada consecuentemente.

III REGISTRO DE LA ICUE A EFECTOS DE SEGURIDAD

20. Se establecerá un registro central en la sede. Todo servicio administrativo del SEAE que maneje ICUE contará con un registro competente, subordinado al registro central, con el fin de garantizar que la ICUE se maneje de conformidad con las disposiciones de la presente Decisión. Los registros se constituirán como zonas de acceso restringido tal y como se definen en el anexo A.

Cada Delegación de la Unión creará su propio registro de ICUE.

La Autoridad de Seguridad del SEAE designará un jefe de registro de esos registros.

21. A efectos de la presente Decisión, por registro a efectos de seguridad (en lo sucesivo, «registro») se entenderá la aplicación de procedimientos que registren el ciclo de vida de la información de que se trate, incluida su difusión y destrucción. En el caso de un SIC, los procedimientos de registro podrán llevarse a cabo mediante procesos dentro del propio SIC.

22. Todo material clasificado de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y superior se inscribirá a su entrada o salida de un servicio administrativo, incluidas las Delegaciones de la Unión. La información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» se inscribirá en registros especiales.

23. El registro central será, en la sede del SEAE, el punto principal de entrada y salida para los intercambios de información clasificada con terceros Estados y organizaciones internacionales. Llevará un registro de todos esos intercambios.

24. La Autoridad de Seguridad del SEAE aprobará unas directrices de seguridad sobre el registro de ICUE a efectos de seguridad, de conformidad con el artículo 14 de la presente Decisión.

Registros «TRÈS SECRET UE/EU TOP SECRET»

25. En la sede del SEAE se establecerá un registro central que actuará como principal organismo receptor y emisor de la información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET». Cuando proceda, podrán designarse registros secundarios para manejar dicha información.

26. Los registros secundarios no podrán transmitir documentos «TRÈS SECRET UE/EU TOP SECRET» directamente a otros registros secundarios dependientes del mismo registro central «TRÈS SECRET UE/EU TOP SECRET» ni al exterior sin la aprobación expresa por escrito de este último.

IV. COPIA Y TRADUCCIÓN DE DOCUMENTOS CLASIFICADOS DE LA UE

27. Los documentos «TRÈS SECRET UE/EU TOP SECRET» solo podrán copiarse o traducirse con el consentimiento previo por escrito del originador.

28. Cuando el originador de documentos clasificados de grado «SECRET UE/EU SECRET» o inferior no haya impuesto ninguna restricción a su copia o traducción, estos documentos podrán copiarse o traducirse por orden de su poseedor.

29. Las medidas de seguridad aplicables a los documentos originales serán aplicables a sus copias y traducciones. Solo podrá realizar copias de documentos con clasificación «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior el (sub) registro pertinente utilizando una fotocopiadora segura. Las copias deberán registrarse.

V. TRANSPORTE DE ICUE

30. El transporte de ICUE estará sujeto a las medidas de protección que se enuncian en los puntos 32 a 42. Cuando se transmita ICUE por medios electrónicos, y no obstante lo dispuesto en el artículo 7, apartado 4, del anexo A, las medidas de protección que figuran a continuación se complementarán con las debidas contramedidas técnicas que prescriba la Autoridad de Seguridad del SEAE, a fin de reducir al mínimo el riesgo de pérdida o compromiso.

31. La Autoridad de Seguridad del SEAE dictará instrucciones para el transporte de ICUE conforme a la presente Decisión.

Dentro de un edificio o grupo independiente de edificios

32. La ICUE que se transporte dentro de un mismo edificio o grupo independiente de edificios irá cubierta, para evitar que se vea su contenido.

33. Dentro de un edificio o grupo independiente de edificios, la información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» se transportará por personas debidamente habilitadas en sobre sellado en el que se indique únicamente el nombre del destinatario.

Dentro de la UE

34. La ICUE que se transporte entre edificios o locales de la UE irá empaquetada de forma que quede protegida de una revelación no autorizada.

35. El transporte de información clasificada de grado «SECRET UE/EU SECRET» o inferior dentro de la UE se efectuará por uno de los siguientes medios:

a) correo diplomático, oficial o militar, según proceda;

b) transporte en mano, siempre que:

i) la ICUE no deje de obrar en poder del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el anexo A II;

ii) la ICUE no se abra durante el camino ni se lea en lugares públicos;

iii) el portador esté habilitado en el grado correspondiente y haya sido instruido sobre sus responsabilidades en materia de seguridad;

iv) se entregue al portador un certificado de correo cuando sea necesario.

c) servicios postales o servicios de mensajería comercial, siempre que:

i) hayan sido aprobados por la ANS competente de conformidad con las disposiciones legales y reglamentarias nacionales; y

ii) apliquen medidas de protección adecuadas de conformidad con los requisitos mínimos que se establezcan en las directrices de seguridad a que se refiere el artículo 21, apartado 1, de la presente Decisión.

Si el transporte se efectúa de un Estado miembro a otro, las disposiciones de la letra c) se aplicarán únicamente a la información clasificada con el grado «CONFIDENTIEL UE/EU CONFIDENTIAL».

36. El material clasificado de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y de grado «SECRET UE/EU SECRET» (por ejemplo, equipo o maquinaria) que no pueda transportarse por los medios indicados en el apartado 34 deberá ser transportado como carga por empresas comerciales de transporte con arreglo a lo dispuesto en el anexo A V.

37. El transporte de información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» entre edificios o locales de la UE se efectuará por correo diplomático, oficial o militar, según proceda.

Desde la UE al territorio de un tercer Estado o entre entidades de la UE en terceros Estados

38. La ICUE que se transporte desde la UE al territorio de un tercer Estado, o entre entidades de la UE en terceros Estados, irá empaquetada de forma que quede protegida de una revelación no autorizada.

39. El transporte de información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y «SECRET UE/EU SECRET» desde la UE al territorio de un tercer Estado, y de cualquier ICUE clasificada «SECRET UE/EU SECRET» entre entidades de la UE en terceros Estados, se efectuará por uno de los siguientes medios:

a) correo diplomático o militar;

b) transporte en mano, siempre que:

i) el paquete lleve sello oficial, o por sus características indique que se trata de un envío oficial, y no debe someterse a controles aduaneros o de seguridad;

ii) el portador lleve un certificado de correo, con mención específica del paquete, que le autorice a transportarlo;

iii) la ICUE no deje de obrar en poder del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el anexo A II;

iv) la ICUE no se abra durante el camino ni se lea en lugares públicos; y

v) el portador esté habilitado en el grado correspondiente y haya sido instruido sobre sus responsabilidades en materia de seguridad.

40. El transporte de información clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y de grado «SECRET UE/UE SECRET» cedida por la UE a un tercer Estado o a una organización internacional deberá atenerse a las disposiciones pertinentes de un acuerdo de seguridad de la información o de un acuerdo administrativo conforme al artículo 10, apartado 2, del anexo A.

41. La información clasificada de grado «RESTREINT UE/EU RESTRICTED» también podrá ser transportada desde la UE al territorio de un Estado miembro por servicios postales o servicios de mensajería comercial.

42. El transporte de información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» desde la UE hasta el territorio de un tercer Estado, o entre entidades de la UE en terceros Estados, se efectuará por correo militar o diplomático.

VI. DESTRUCCIÓN DE ICUE

43. Los documentos clasificados de la UE que hayan dejado de ser necesarios podrán destruirse, sin perjuicio de las correspondientes normas sobre archivos.

44. Los documentos sujetos a registro de conformidad con el artículo 7, apartado 2, del anexo A, serán destruidos por el registro competente por orden de su poseedor o de una autoridad competente. Los libros de registro y cualquier información relacionada con el registro se actualizarán en consecuencia.

45. Cuando se trate de documentos clasificados de grado «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», la destrucción se realizará en presencia de un testigo, que deberá estar habilitado como mínimo para el grado de clasificación del documento que se vaya a destruir.

46. El encargado del registro, y el testigo en caso de que se requiera su presencia, firmarán un certificado de destrucción, que se archivará en el registro. El registro conservará los certificados de destrucción de los documentos de grado «TRÈS SECRET UE/EU TOP SECRET» durante diez años como mínimo y de los documentos de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» y «SECRET UE/EU SECRET» durante cinco años como mínimo.

47. Los documentos clasificados, incluidos los de grado «RESTREINT UE/EU RESTRICTED», se destruirán por medio de métodos que cumplan las normas de la UE pertinentes o normas equivalentes o que hayan sido homologados por los Estados miembros de conformidad con las normas técnicas nacionales, a fin de impedir su reconstrucción total o parcial.

48. La destrucción de los soportes de almacenamiento informático utilizados para la ICUE se realizará de conformidad con los procedimientos aprobados por la Autoridad de Seguridad del SEAE.

VII. INSPECCIONES DE SEGURIDAD

Inspecciones de seguridad del SEAE

49. De conformidad con el artículo 16 de la presente Decisión, las inspecciones de seguridad del SEAE serán de los siguientes tipos:

a) inspecciones generales de seguridad, con el objetivo de evaluar el nivel general de seguridad de la sede del SEAE, las Delegaciones de la Unión y todos los locales dependientes o relacionados, y, en especial, evaluar la efectividad de las medidas de seguridad aplicadas para proteger los intereses de seguridad del SEAE;

b) inspecciones de seguridad de la ICUE, con el objetivo de evaluar, normalmente con vistas a una acreditación, la efectividad de las medidas aplicadas para proteger la ICUE en la sede del SEAE y en las Delegaciones de la Unión.

En particular, las inspecciones se realizarán, entre otros fines, para:

i) asegurarse de que se apliquen las normas mínimas para la protección de la ICUE establecidas en la presente Decisión;

ii) destacar la importancia de la seguridad y de una efectiva gestión del riesgo en las entidades inspeccionadas;

iii) recomendar contramedidas que permitan paliar los efectos específicos de la pérdida de confidencialidad, integridad o disponibilidad de la información clasificada; y

iv) reforzar los programas de formación y de concienciación en cuestiones de seguridad que ya realicen las autoridades de seguridad.

Realización de las inspecciones de seguridad del SEAE y elaboración de informes

50. Las inspecciones de seguridad del SEAE serán realizadas por un equipo de inspección de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, que contará, cuando sea necesario, con la asistencia de expertos en seguridad de otras instituciones de la UE o de los Estados miembros.

El equipo inspector tendrá acceso a todos los locales, en particular a los registros y puntos de presencia de los SIC, en los que se maneje ICUE.

51. Las inspecciones de seguridad del SEAE en las Delegaciones de la Unión podrán realizarse, cuando sea necesario, con la asistencia de funcionarios de seguridad de las embajadas de los Estados miembros en terceros países.

52. Antes del término de cada año natural, la Autoridad de Seguridad del SEAE adoptará el programa de inspecciones de seguridad para el año siguiente.

53. En caso necesario, la Autoridad de Seguridad del SEAE podrá organizar inspecciones de seguridad no previstas en el programa anterior.

54. Al término de la inspección de seguridad se presentarán a la entidad inspeccionada las principales conclusiones y recomendaciones. Seguidamente, el equipo de inspección deberá redactar un informe de inspección. Cuando se hayan propuesto medidas correctoras y recomendaciones, el informe incluirá datos suficientes que avalen sus conclusiones. El informe se remitirá a la Autoridad de Seguridad del SEAE, al director del Centro de Respuesta a las Crisis, por lo que respecta a las inspecciones de seguridad en las Delegaciones de la Unión, y al responsable de la entidad inspeccionada.

Se elaborará un informe periódico, bajo la responsabilidad de la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, para destacar las principales enseñanzas extraídas de las inspecciones realizadas a lo largo de un período determinado; el informe será examinado por el Comité de Seguridad del SEAE.

Realización de inspecciones de seguridad en los órganos y organismos de la UE establecidos en virtud del título V, capítulo 2, del TUE, y elaboración de informes

55. Cuando proceda, la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE podrá designar expertos colaboradores para participar en equipos conjuntos de inspección de la UE que lleven a cabo inspecciones en los órganos y organismos de la UE establecidos en virtud del título V, capítulo 2, del TUE.

Lista de control para las inspecciones de seguridad del SEAE

56. Corresponderá a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE elaborar y actualizar una lista de control para las inspecciones de seguridad que recoja los puntos que deban comprobarse en el curso de una inspección de seguridad del SEAE. Esta lista se remitirá al Comité de Seguridad del SEAE.

57. Durante la inspección, la información para completar la lista de control se obtendrá, en particular, de los encargados de la gestión de seguridad de la entidad inspeccionada. Una vez completada con las respuestas detalladas, la lista de control se clasificará de común acuerdo con la entidad inspeccionada. No formará parte del informe de inspección.

ANEXO A IV

PROTECCIÓN DE LA ICUE MANEJADA EN LOS SIC

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 8 del anexo A.

2. Las siguientes propiedades y conceptos relativos a la garantía de la información (GI) se consideran esenciales para la seguridad y el correcto funcionamiento de las operaciones realizadas en los sistemas de información y comunicación (SIC):

Autenticidad:	la garantía de que la información es verídica y procede de fuentes de buena fe.
Disponibilidad:	la propiedad de ser accesible y utilizable en el momento que lo requiera una entidad autorizada.
Confidencialidad:	la propiedad de la información de no ser revelada a personas, organismos ni procesos no autorizados;
Integridad:	la propiedad de salvaguardar la exactitud y completitud de la información y los activos;
No repudio:	la capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente.

II PRINCIPIOS DE LA GARANTÍA DE LA INFORMACIÓN

3. Las disposiciones que se establecen a continuación constituyen el punto de partida para garantizar la seguridad de todo sistema que maneje ICUE por parte de un SIC. Los requisitos detallados para dar cumplimiento a las presentes disposiciones se definirán en directrices de seguridad para la garantía de la información (GI).

Gestión del riesgo de seguridad

4. La gestión del riesgo de seguridad será parte integrante de la definición, desarrollo, funcionamiento y mantenimiento de los SIC. La gestión del riesgo (evaluación, tratamiento, aceptación y comunicación) se llevará a cabo como un proceso iterativo y de forma conjunta por parte de los representantes de los propietarios del sistema, las autoridades del proyecto, las autoridades operativas y las autoridades responsables de la aprobación de la seguridad, recurriendo a un método de evaluación del riesgo que haya demostrado su eficacia y sea transparente y plenamente comprensible. El alcance del SIC y de sus activos estará claramente definido ya desde el comienzo del proceso de gestión del riesgo.

5. Las autoridades competentes del SEAE examinarán las amenazas potenciales para el SIC y elaborarán evaluaciones precisas de las amenazas, que reflejen el entorno operativo del momento y que mantendrán actualizadas. Actualizarán continuamente sus conocimientos de las cuestiones relativas a la vulnerabilidad y revisarán periódicamente la evaluación de la vulnerabilidad para hacer frente al entorno cambiante de las tecnologías de la información.

6. La gestión del riesgo de seguridad tendrá por objetivo aplicar un conjunto de medidas de seguridad que constituyan un equilibrio satisfactorio entre las necesidades de los usuarios y el riesgo de seguridad residual.

7. Los requisitos específicos, la escala y el grado de detalle determinados por la Autoridad de Acreditación de Seguridad (AAS) pertinente para acreditar un SIC serán proporcionales al riesgo evaluado, teniendo en cuenta todos los factores pertinentes, con inclusión del grado de clasificación de la ICUE manejada por el SIC. La acreditación incluirá una declaración formal sobre el riesgo residual y la aceptación de dicho riesgo por parte de una autoridad competente.

Seguridad a lo largo del ciclo de vida del SIC

8. Garantizar la seguridad constituirá un requisito a lo largo de todo el ciclo de vida del SIC, desde su comienzo hasta su retirada del servicio.

9. Para cada fase del ciclo de vida de un sistema, se determinará el papel y la interacción de todo participante en un SIC con respecto a su seguridad.

10. Todo SIC, incluidas sus medidas de seguridad de carácter técnico y no técnico, será objeto de pruebas de seguridad durante su proceso de acreditación, para asegurarse de que se obtiene el nivel adecuado de garantía de las medidas de seguridad aplicadas y verificar que el sistema esté correctamente aplicado, integrado y configurado.

11. Se realizarán periódicamente evaluaciones, inspecciones y exámenes de seguridad durante el funcionamiento y el mantenimiento del SIC y cuando se produzcan circunstancias excepcionales.

12. La documentación de seguridad de un SIC irá evolucionando a lo largo de su ciclo de vida como parte integrante del proceso de gestión de la configuración y del cambio.

Mejores prácticas

13. El SEAE colaborará con la SGC, la Comisión y los Estados miembros en el desarrollo de mejores prácticas para la protección de la ICUE manejada en los SIC. Las directrices sobre las mejores prácticas establecerán medidas de seguridad técnicas, físicas, de organización y de procedimiento para los SIC, de probada eficacia para contrarrestar determinadas amenazas y vulnerabilidades.

14. La protección de la ICUE manejada en los SIC se basará en las enseñanzas extraídas por las entidades que intervengan en la GI tanto dentro como fuera de la UE.

15. La difusión y ulterior aplicación de las mejores prácticas contribuirán a lograr un nivel equivalente de garantía en los distintos SIC que manejen ICUE y que funcionen en el SEAE.

Defensa en profundidad

16. Al objeto de paliar los riesgos para los SIC, se aplicará una serie de medidas de seguridad de carácter técnico y no técnico, organizadas a modo de defensa en barreras sucesivas. Esas barreras de defensa incluirán:

    a) *disuasión*: medidas de seguridad destinadas a desalentar a los adversarios que planeen un ataque a un SIC;

    b) *prevención*: medidas de seguridad destinadas a impedir u obstaculizar un ataque a un SIC;

    c) *detección*: medidas de seguridad destinadas a descubrir si se ha producido un ataque a un SIC;

    d) *resiliencia*: medidas de seguridad destinadas a limitar las consecuencias de un ataque a un bloque mínimo de información o de activos de un SIC y a impedir mayores daños; y

    e) *recuperación*: medidas de seguridad destinadas a volver al estado anterior de seguridad del SIC.

    El grado de rigor y aplicabilidad de estas medidas de seguridad se determinará mediante una evaluación del riesgo.

17. Las autoridades competentes del SEAE se asegurarán de poder responder a incidentes que puedan trascender el ámbito de las organizaciones o las fronteras nacionales, con el fin de coordinar las respuestas y compartir información sobre dichos incidentes y los riesgos conexos (capacidades de respuesta para urgencias informáticas).

Principio de minimalidad y privilegios mínimos

18. Únicamente se pondrán en marcha las funciones, dispositivos y servicios necesarios para cubrir las necesidades operativas, con el fin de evitar riesgos innecesarios.

19. Los usuarios de los SIC y los procesos automáticos solo obtendrán el acceso, los privilegios o los permisos que necesiten para realizar su cometido, con el fin de limitar los daños resultantes de accidentes, errores o uso no autorizado de recursos de los SIC.

20. Los procedimientos de registro que efectúe un SIC, cuando sea preciso, se verificarán como parte del proceso de acreditación.

Concienciación de la GI

21. La conciencia de los riesgos y de las medidas de seguridad existentes constituye la primera línea de defensa de la seguridad de los SIC. En particular, todas las personas que intervengan en el ciclo de vida de un SIC, incluidos sus usuarios, deberán ser conscientes de:

    a) que los fallos de seguridad pueden perjudicar seriamente al SIC y a la organización en su conjunto;

    b) los posibles daños a terceros que puedan derivarse de la interconectividad y la interdependencia; y

    c) que son responsables de la seguridad del SIC y se les pedirán cuentas según la función que desempeñen en los sistemas y procesos.

22. Para garantizar que sean conscientes de las responsabilidades que conlleva la seguridad, será obligatoria la formación y concienciación sobre la GI para todo el personal implicado, tanto los altos directivos como los usuarios de SIC.

Evaluación y aprobación de los productos de seguridad informática

23. El grado de confianza necesario en las medidas de seguridad, definido como nivel de garantía, se determinará con arreglo al resultado del proceso de gestión del riesgo y en consonancia con las correspondientes políticas y directrices de seguridad.

24. El nivel de garantía se verificará recurriendo a procedimientos y metodologías reconocidos internacionalmente o aprobados en el plano nacional. Aquí se incluyen principalmente la evaluación, los controles y las auditorías.

25. Los productos criptográficos de protección de la ICUE serán evaluados y aprobados por una Autoridad de Certificación Criptológica (ACC) de un Estado miembro.

26. Antes de recomendarlos para su aprobación por la ACC del SEAE, de conformidad con el artículo 8, apartado 5, de la presente Decisión, dichos productos criptográficos deberán superar una segunda evaluación realizada por la autoridad debidamente acreditada (ADA) de un Estado miembro que no haya participado en el diseño o fabricación del equipo considerado. El grado de detalle exigido en la segunda evaluación dependerá del grado máximo de clasificación de la ICUE que se prevé proteger con dichos productos.

27. Cuando ello esté justificado por motivos operativos específicos, la ACC del SEAE podrá, previa recomendación del Comité de Seguridad del Consejo, conceder una dispensa del cumplimiento de los requisitos recogidos en los apartados 25 o 26 y otorgar una aprobación provisional durante un período específico, de conformidad con el artículo 8, apartado 5, de la presente Decisión.

28. Una ADA será una ACC de un Estado miembro que haya sido acreditada con arreglo a criterios objetivos establecidos por el Consejo para realizar la segunda evaluación de los productos criptológicos de protección de la ICUE.

29. El Alto Representante aprobará una política de seguridad sobre la cualificación y aprobación de productos de seguridad informática no criptográficos.

Transmisión dentro de zonas de acceso restringido

30. No obstante las disposiciones de la presente Decisión, cuando la transmisión de ICUE se limite a zonas de acceso restringido o a zonas administrativas, podrá utilizarse la difusión no cifrada, o cifrada en un nivel inferior, con base en el resultado de un proceso de gestión del riesgo y previa aprobación de la AAS.

Interconexión segura de los SIC

31. A los efectos de la presente Decisión, por interconexión se entenderá la conexión directa entre dos o más sistemas de informáticos para compartir datos y otros recursos de información (por ejemplo, comunicación) de forma unidireccional o multidireccional.

32. Todo SIC tratará como no fiable cualquier sistema informático interconectado, y aplicará medidas protectoras para controlar el intercambio de información clasificada.

33. Para todas las interconexiones de un SIC con otro sistema informático se observarán los siguientes requisitos básicos:

    a) las autoridades competentes enunciarán y aprobarán los requisitos operativos o de servicio de dichas interconexiones;

    b) la interconexión se someterá a un proceso de gestión del riesgo y acreditación y necesitará la aprobación de las autoridades de acreditación de seguridad competentes; y

    c) se pondrán en marcha servicios de protección del perímetro de todos los SIC.

34. No habrá interconexión entre un SIC acreditado y una red desprotegida o pública, salvo cuando el SIC tenga instalado a tal fin un servicio de protección de perímetro aprobado, que actúe entre el SIC y la red desprotegida o pública. Las medidas de seguridad de tales interconexiones serán examinadas por la autoridad de garantía de la información (AGI) competente y aprobadas por la autoridad de acreditación de seguridad competente.

    Cuando la red desprotegida o pública se utilice únicamente para el transporte, y los datos estén cifrados con un producto criptográfico aprobado de conformidad con el artículo 8, apartado 5, de la presente Decisión, se considerará que la conexión no es una interconexión.

35. Quedarán prohibidas las interconexiones directas o dispuestas en cascada de un SIC acreditado para manejar información clasificada de grado «TRÈS SECRET UE/EU TOP SECRET» con redes públicas o desprotegidas.

Soportes de almacenamiento informático

36. Los soportes de almacenamiento informático se destruirán con arreglo a un procedimiento aprobado por la Autoridad de Seguridad del SEAE.

37. La reutilización, la reducción del grado de clasificación y la desclasificación de los soportes de almacenamiento informático se efectuarán de conformidad con las directrices de seguridad establecidas con arreglo al artículo 8, apartado 2, de la presente Decisión.

Circunstancias de emergencia

38. No obstante lo dispuesto en la presente Decisión, podrán aplicarse, durante un período de tiempo limitado, los procedimientos específicos que se describen a continuación en casos de emergencia, por ejemplo, en situaciones de crisis, conflicto o guerra, inminentes o reales, o en circunstancias operativas excepcionales.

39. La ICUE podrá transmitirse utilizando productos criptológicos que hayan sido certificados para un grado de clasificación inferior o no estén encriptados, con el consentimiento de la autoridad competente, si resulta evidente que un retraso podría causar un daño superior al que acarree la revelación del material clasificado y si:

    a) el emisor y el receptor carecen de los medios de cifrado requeridos o carecen de todo medio de cifrado; y

    b) el material clasificado no puede transmitirse a tiempo por otros medios.

40. En las circunstancias expuestas en el punto 39, la información clasificada transmitida no llevará ninguna marca ni indicación que la distinga de la información no clasificada o que pueda protegerse mediante un producto criptológico disponible. Se notificará sin demora a los receptores el grado de clasificación, recurriendo a otros medios.

41. Si hubiera que recurrir a lo dispuesto en el apartado 39, se presentará posteriormente un informe a la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y, a través de ella, al Comité de Seguridad del SEAE. En dicho informe se indicarán, como mínimo, el emisor, el receptor y el originador de cada ICUE.

III GARANTÍA DE LA INFORMACIÓN: FUNCIONES Y AUTORIDADES

42. El SEAE establecerá las funciones en materia de GI que se indican seguidamente. Estas funciones no necesitan ser desempeñadas por organismos específicos y únicos. Tendrán cometidos separados. Sin embargo, dichas funciones y sus responsabilidades conexas podrán combinarse o integrarse en el mismo servicio administrativo, o dividirse entre varios de ellos, siempre que se eviten los conflictos internos de intereses o de funciones.

Autoridad de Garantía de la Información

43. Corresponderá a la Autoridad de Garantía de la Información (AGI):

a) establecer directrices de seguridad relativas a la GI y supervisar su eficacia y pertinencia;

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

c) garantizar que las medidas de GI seleccionadas para proteger la ICUE cumplan las directrices que rigen su idoneidad y selección;

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

e) coordinar la formación y la concienciación respecto de la GI;

f) consultar al proveedor del sistema, a los interlocutores en el ámbito de la seguridad y a los representantes de los usuarios sobre las directrices de seguridad relativas a la GI; y

g) velar por que se disponga de los conocimientos técnicos necesarios en la subsección especializada del Comité de Seguridad del SEAE para cuestiones de GI.

Autoridad TEMPEST

44. Corresponderá a la autoridad TEMPEST garantizar que los SIC cumplan las políticas y directrices TEMPEST. La autoridad TEMPEST aprobará contramedidas para instalaciones y productos destinados a proteger la ICUE de un determinado grado de clasificación dentro de su entorno operativo.

Autoridad de Certificación Criptológica

45. Corresponderá a la ACC garantizar que los productos criptográficos cumplan las correspondientes directrices criptológicas. Dará su aprobación a los productos criptográficos para tratar ICUE de un determinado grado de clasificación dentro de su entorno operativo.

Autoridad de Distribución Criptológica

46. Corresponderá a la ADC:

a) gestionar y contabilizar el material criptológico de la UE;

b) garantizar que se apliquen los procedimientos adecuados y se establezcan los cauces pertinentes para rendir cuentas de todo el material criptográfico de la UE, así como para que su manejo, almacenamiento y distribución; y

c) garantizar la transferencia del material criptológico de la UE entre las personas o servicios que lo empleen.

Autoridad de Acreditación de Seguridad

47. Corresponderá a la Autoridad de Acreditación de Seguridad (AAS) de cada sistema:

a) velar por que los SIC cumplan las directrices de seguridad pertinentes, expedir una declaración de aprobación a los SIC para manejar ICUE de un determinado grado de clasificación en su entorno operativo en la que se declaren las condiciones de la acreditación y los criterios aplicables para exigir una nueva aprobación;

b) establecer un proceso de acreditación de seguridad, de conformidad con las directrices pertinentes, que enuncie claramente las condiciones de aprobación de los SIC bajo su autoridad;

c) definir una estrategia de acreditación de seguridad que indique el grado de detalle para el proceso de acreditación según el nivel de garantía requerido;

d) examinar y aprobar la documentación de seguridad, incluidas las declaraciones de gestión del riesgo y de riesgo residual, las declaraciones de requisitos específicos de seguridad del sistema, la documentación relativa a la verificación de la aplicación de la seguridad y los procedimientos operativos de seguridad y asegurarse de que se cumplan las normas y directrices de seguridad del SEAE;

e) comprobar la aplicación de las medidas de seguridad en relación con los SIC realizando o patrocinando evaluaciones de seguridad, inspecciones o exámenes;

f) aprobar los criterios de seguridad (por ejemplo, los grados de habilitación del personal) para puestos delicados en relación con los SIC;

g) refrendar la selección de productos criptológicos y TEMPEST aprobados para dotar de seguridad a los SIC;

h) aprobar la interconexión de un SIC a otro SIC o, cuando proceda, participar en la aprobación conjunta de dicha interconexión; y

i) consultar al proveedor del sistema, a los actores en el ámbito de la seguridad y a los representantes de los usuarios respecto de la gestión del riesgo, en particular del riesgo residual, así como sobre las condiciones de la declaración de aprobación.

48. Corresponderá a la AAS del SEAE la acreditación de todos los SIC que funcionen dentro del ámbito del SEAE.

Panel de Acreditación de Seguridad

49. Un Panel de Acreditación de Seguridad (PAS) conjunto se encargará de la acreditación de los SIC que sean competencia tanto de la AAS del SEAE como de las AAS de los Estados miembros. Estará integrado por un representante de la AAS de cada Estado miembro y asistirá a él un representante de la AAS de la SGC y de la Comisión. Se invitará a asistir a otras entidades conectadas a un SIC, cuando dicho sistema se someta a debate.

El PAS estará presidido por un representante de la AAS del SEAE. Se pronunciará por consenso de los representantes de las AAS de las instituciones, de los Estados miembros y de otras entidades conectados al SIC de que se trate. Elaborará informes periódicos sobre sus actividades, destinados al Comité de Seguridad del SEAE y le comunicará todas las declaraciones de acreditación.

Autoridad Operativa de Garantía de la Información

50. Corresponderá a la Autoridad Operativa de Garantía de la Información (AOGI) de cada sistema:

a) elaborar documentación de seguridad en consonancia con las directrices de seguridad, en particular con los requisitos específicos de seguridad del sistema, incluida la declaración sobre el riesgo residual, los procedimientos operativos de seguridad y el plan criptológico 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 la enunciación de requisitos específicos de seguridad del sistema y garantizar que su instalación y mantenimiento sean seguros, en colaboración con la autoridad TEMPEST;

d) supervisar el cumplimiento y aplicación de los procedimientos operativos de seguridad y, cuando proceda, delegar las competencias sobre la seguridad operativa en el propietario del sistema;

e) gestionar y manejar productos criptológicos, garantizando la custodia de los artículos criptológicos y 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 el riesgo, cuando así lo requiera la Autoridad de Acreditación de Seguridad (AAS);

g) proporcionar formación sobre la GI específica para SIC;

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

ANEXO A V

SEGURIDAD INDUSTRIAL

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 9 del anexo A, así como disposiciones generales en materia de seguridad aplicables a las sociedades industriales u otro tipo de entidades en las negociaciones precontractuales y durante toda la vigencia de los contratos clasificados adjudicados por el SEAE.

2. La Autoridad de Seguridad del SEAE aprobará unas directrices sobre seguridad industrial que definan, en particular, requisitos detallados en relación con las habilitaciones de seguridad de establecimiento, las cláusulas sobre aspectos de la seguridad, las visitas y la transmisión y el transporte de ICUE.

II ELEMENTOS DE SEGURIDAD EN UN CONTRATO CLASIFICADO

Guía de clasificación de seguridad

3. Antes de publicar una convocatoria de licitación o adjudicar un contrato clasificado, el SEAE, como autoridad contratante, determinará la clasificación de seguridad de toda información que deba proporcionarse a los licitadores y contratistas, así como la clasificación de seguridad de toda información que haya de producir el contratista. Para ello, el SEAE elaborará una guía de clasificación de seguridad que deberá emplearse en la ejecución del contrato.

4. Para determinar la clasificación de seguridad de los diversos elementos de un contrato clasificado se aplicarán los principios siguientes:

   a) al elaborar una guía de clasificación de seguridad, el SEAE tendrá en cuenta todos los aspectos de seguridad pertinentes, incluida la clasificación de seguridad atribuida a la información que se facilite y apruebe para ser utilizada en el contrato en cuestión por el originador de la información;

   b) el grado global de clasificación del contrato no podrá ser inferior al grado más elevado de clasificación de cualquiera de sus elementos; y

   c) cuando proceda, en caso de que se produzca algún cambio en relación con la clasificación de la información producida por los contratistas o que se les haya facilitado en la ejecución de un contrato, y cuando se introduzca cualquier cambio ulterior en la guía de clasificación de seguridad, el SEAE actuará de enlace con las ANS o las ASD de los Estados miembros o con cualquier otra autoridad nacional de seguridad afectada.

Cláusula sobre aspectos de la seguridad

5. Los requisitos de seguridad específicos de un contrato se describirán en una cláusula sobre aspectos de la seguridad, la cual, cuando proceda, incluirá una guía de clasificación de seguridad y será parte integrante del contrato o subcontrato clasificado.

6. La cláusula sobre aspectos de la seguridad incluirá asimismo disposiciones que exijan del contratista o subcontratista el cumplimiento de las normas mínimas que se establecen en la presente Decisión. El incumplimiento de dichas normas mínimas podrá ser motivo suficiente para la rescisión del contrato.

Instrucciones de seguridad de un programa o proyecto

7. En función del ámbito de los programas o proyectos que conlleven acceso a ICUE o su manejo o almacenamiento, la autoridad contratante designada para gestionar el programa o proyecto podrá dictar unas instrucciones de seguridad específicas del programa o proyecto. Estas instrucciones requerirán la aprobación de las ANS o las ASD de los Estados miembros, o de cualquier otra autoridad de seguridad competente, que participen en un determinado proyecto o programa, y podrán contener requisitos de seguridad adicionales.

III HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO

8. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE solicitará a la ANS, a la ASD o a cualquier otra autoridad de seguridad competente del Estado miembro afectado que conceda una habilitación de seguridad de establecimiento para indicar, de conformidad con las disposiciones legales y reglamentarias nacionales, que una sociedad industrial u otro tipo de entidad puede proteger dentro de sus instalaciones la ICUE del grado de clasificación que corresponda («CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET»). No se concederá acceso a ICUE a contratistas, subcontratistas, contratistas potenciales o subcontratistas potenciales hasta que se haya comunicado al SEAE una prueba de habilitación de seguridad de establecimiento.

9. Cuando proceda, el SEAE, como autoridad contratante, comunicará a la ANS o a la ASD competente o a cualquier otra autoridad de seguridad competente que es necesario contar con una habilitación de seguridad de establecimiento en la fase precontractual o para la ejecución del contrato. En la fase precontractual, será necesaria una habilitación de seguridad de establecimiento o una HPS cuando durante el proceso de licitación deba facilitarse información clasificada de los grados «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET».

10. El SEAE, como autoridad contratante, no adjudicará un contrato clasificado al licitador seleccionado hasta haber recibido de la ANS o de la ASD o de cualquier otra autoridad de seguridad competente del Estado miembro en que esté registrado el contratista o subcontratista confirmación de que se ha expedido a este la habilitación de seguridad de establecimiento adecuada.

11. El SEAE, como autoridad contratante, solicitará a la ANS o la ASD o a cualquier otra autoridad de seguridad competente que haya expedido una habilitación de seguridad de establecimiento que le comunique cualquier información desfavorable que afecte a dicha habilitación. En el caso de los subcontratos, se informará al respecto a la ANS, a la ASD o a cualquier otra autoridad de seguridad competente.

12. La retirada de una habilitación de seguridad de establecimiento por parte de la ANS, de la ASD o de cualquier otra autoridad de seguridad competente constituirá motivo suficiente para que el SEAE, como autoridad contratante, rescinda un contrato clasificado o excluya a un licitador de la licitación.

IV. HABILITACIONES DE SEGURIDAD DE PERSONAL PARA EL PERSONAL DE LOS CONTRATISTAS

13. Todo el personal que trabaje para contratistas y necesite acceder a ICUE clasificada de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior deberá ser adecuadamente habilitado y acreditar la necesidad de conocer dicha información. Aunque no se requiere una habilitación de seguridad del personal para acceder a ICUE de grado «RESTREINT UE/EU RESTRICTED», dicho acceso se supeditará a la necesidad de conocer.

14. Las solicitudes de habilitaciones de seguridad del personal para el personal de los contratistas deberán presentarse a la ANS o la ADS responsable de la entidad.

15. El SEAE indicará a los contratistas que deseen emplear a un nacional de un tercer Estado para un puesto que requiera acceso a ICUE que corresponde a la ANS o a la ADS del Estado miembro en el que esté ubicada e integrada la entidad contratante determinar si se puede conceder a esa persona acceso a dicha información de conformidad con la presente Decisión, y confirmar que debe recabarse el consentimiento del originador antes de conceder el acceso.

V. CONTRATOS Y SUBCONTRATOS CLASIFICADOS

16. Cuando se facilite ICUE a un licitador en la fase precontractual, el pliego de condiciones generales deberá contener una cláusula que obligue a los licitadores que no presenten ofertas o que no resulten seleccionados a devolver toda la documentación clasificada en un plazo determinado.

17. Una vez que se haya adjudicado un contrato o subcontrato clasificado, el SEAE, como autoridad contratante, notificará a la ANS, a la ASD o a cualquier otra autoridad de seguridad competente del contratista o subcontratista las disposiciones de seguridad del contrato clasificado.

18. En caso de rescisión o finalización de un contrato de este tipo, el SEAE, como autoridad contratante (o la ANS, la ASD o cualquier otra autoridad de seguridad competente, según proceda, en el caso de una subcontratación), lo notificará sin demora a la ANS, a la ASD o a cualquier otra autoridad de seguridad competente del Estado miembro en que esté registrado el contratista o subcontratista.

19. Por regla general, el contratista o subcontratista estará obligado a devolver a la autoridad contratante, tras la rescisión o finalización del contrato o subcontrato clasificado, toda la ICUE que obre en su poder.

20. La cláusula sobre aspectos de la seguridad establecerá disposiciones específicas para la eliminación de ICUE durante la ejecución del contrato o tras la rescisión o finalización de este.

21. Cuando el contratista o subcontratista esté autorizado a conservar ICUE tras la rescisión o finalización de un contrato, seguirán siendo de aplicación las normas mínimas contenidas en la presente Decisión, y el contratista o subcontratista protegerá la confidencialidad de la ICUE.

22. Las condiciones en que un contratista pueda subcontratar se definirán en el pliego de condiciones generales y en el contrato.

23. Antes de subcontratar cualquier parte de un contrato clasificado, el contratista deberá obtener del SEAE, como autoridad contratante, el permiso correspondiente. No podrá adjudicarse un subcontrato a sociedades industriales u otro tipo de entidades registradas en un Estado que no sea miembro de la UE y no haya celebrado un acuerdo de seguridad de la información con esta.

24. El contratista responderá de que todas las actividades subcontratadas se ejecuten de conformidad con las normas mínimas establecidas en la presente Decisión y no transmitirá ICUE a ningún subcontratista sin el previo consentimiento escrito del órgano de contratación.

25. Respecto de la ICUE producida o manejada por el contratista o subcontratista, los derechos que asistan al originador serán ejercidos por la autoridad contratante.

VI. VISITAS EN RELACIÓN CON CONTRATOS CLASIFICADOS

26. Cuando el SEAE, los contratistas o los subcontratistas necesiten acceder a información clasificada de los grados «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET» que se halle en los locales de los otros para la ejecución de un contrato clasificado, se organizarán visitas, en contacto con las ANS, las ASD o con cualquier otra autoridad de seguridad competente. Ello no afectará a la prerrogativa de las ANS o las ASD, en el contexto de proyectos específicos, de acordar un procedimiento que permita organizar directamente dichas visitas.

27. Todos los visitantes deberán estar en posesión de una HPS y tener necesidad de conocer para poder acceder a la ICUE relacionada con el contrato del SEAE.

28. A los visitantes solo se les permitirá el acceso a ICUE que guarde relación con la finalidad de la visita.

VII. TRANSMISIÓN Y TRANSPORTE DE ICUE

29. Por lo que se refiere a la transmisión de ICUE por medios electrónicos, se aplicarán las disposiciones pertinentes del artículo 8 del anexo A y del anexo A IV.

30. Por lo que se refiere al transporte de ICUE, se aplicarán las disposiciones pertinentes del anexo A III, de conformidad con las disposiciones legales y reglamentarias nacionales.

31. Por lo que se refiere al transporte como carga de material clasificado, se aplicarán los siguientes principios para determinar las medidas de seguridad:

    a) la seguridad deberá estar garantizada durante todas las fases del transporte, desde el punto de origen hasta el destino final;

    b) el grado de protección concedido a un envío se determinará en función del grado más elevado de clasificación del material que contenga;

    c) se obtendrá una habilitación de seguridad de establecimiento del grado adecuado para las sociedades encargadas del transporte, si este último implica asimismo el almacenamiento de información clasificada en los locales del contratista. En cualquier caso, el personal que se ocupe del envío deberá estar debidamente habilitado de conformidad con el anexo A I;

    d) antes de efectuar cualquier traslado transfronterizo de material clasificado de los grados «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET UE/EU SECRET», el remitente elaborará un plan de transporte que deberá ser aprobado por el SEAE, si procede en conexión con las ANS o ASD del remitente y el destinatario, o con cualquier otra autoridad de seguridad competente afectada;

e) en la medida de lo posible, los viajes evitarán las paradas intermedias y se completarán con tanta la celeridad como las circunstancias permitan; y

f) siempre que sea posible, se circulará exclusivamente a través de Estados miembros. Solo deberán emplearse itinerarios que atraviesen Estados no miembros de la UE previa autorización del SEAE o de cualquier otra autoridad de seguridad competente tanto del Estado remitente como del Estado destinatario.

VIII. TRANSMISIÓN DE ICUE A CONTRATISTAS ESTABLECIDOS EN TERCEROS ESTADOS

32. La transmisión de ICUE a contratistas y subcontratistas establecidos en terceros Estados con los que esté en vigor un acuerdo de seguridad válido con la UE se hará de conformidad con las medidas de seguridad que adopten de común acuerdo el SEAE, como autoridad contratante, y la ANS o la ASD del tercer Estado afectado en que esté registrado el contratista.

IX. MANEJO Y ALMACENAMIENTO DE INFORMACIÓN CLASIFICADA DE GRADO «RESTREINT UE/EU RESTRICTED»

33. El SEAE, como autoridad contratante, en colaboración con la ANS o la ASD del Estado miembro, según proceda, estará facultada para realizar visitas a los establecimientos de los contratistas o subcontratistas en virtud de disposiciones contractuales, con el fin de cerciorarse de que se aplican las medidas de seguridad adecuadas para la protección de la ICUE de grado «RESTREINT UE/EU RESTRICTED», tal como se haya estipulado en el contrato.

34. En la medida necesaria de conformidad con las disposiciones legales y reglamentarias nacionales, el SEAE, como autoridad contratante, notificará a la ANS, a la ASD o a cualquier otra autoridad de seguridad competente los contratos o subcontratos que contengan información clasificada de grado «RESTREINT UE/EU RESTRICTED».

35. Para los contratos adjudicados por el SEAE que contengan información clasificada de grado «RESTREINT UE/EU RESTRICTED», no se exigirá a los contratistas o subcontratistas ni a su personal una habilitación de seguridad de establecimiento ni una HPS.

36. El SEAE, como autoridad contratante, estudiará las respuestas a las invitaciones a presentar ofertas para los contratos que requieran el acceso a información clasificada de grado «RESTREINT UE/EU RESTRICTED», independientemente de los requisitos relativos a una habilitación de seguridad de establecimiento o una HPS que puedan exigir las disposiciones legales y reglamentarias nacionales.

37. Las condiciones con arreglo a las cuales el contratista pueda subcontratar deberán estar en conformidad con los apartados 22 a 24.

38. Cuando un contrato prevea el manejo de información clasificada de grado «RESTREINT UE/EU RESTRICTED» en un SIC gestionado por un contratista, el SEAE, como autoridad contratante, garantizará que en el contrato o en cualquier posible subcontrato se detallen los requisitos técnicos y administrativos necesarios para la acreditación del SIC, que deberán ser acordes al riesgo evaluado, teniendo en cuenta todos los factores pertinentes. El ámbito de la acreditación de dicho SIC se determinará mediante acuerdo entre la autoridad contratante y la ANS o la ASD competente.

ANEXO A VI

INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 10 del anexo A.

II. MARCOS QUE REGULAN EL INTERCAMBIO DE INFORMACIÓN CLASIFICADA

2. El SEAE podrá intercambiar ICUE con terceros Estados y organizaciones internacionales de conformidad con el artículo 10, apartado 1, del anexo A.

   Para apoyar al AR en el ejercicio de las responsabilidades establecidas en el artículo 218 del TFUE:

   a) el departamento geográfico o temático pertinente del SEAE, en consulta con la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, señalará, cuando proceda, la necesidad de un intercambio de ICUE de larga duración con un tercer Estado o una organización internacional;

   b) la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE, en consulta con el departamento geográfico pertinente del SEAE, presentará al AR, cuando proceda, los proyectos de textos que deban proponerse al Consejo en virtud del artículo 218, apartados 3, 5 y 6, del TFUE;

   c) la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE asistirá al AR en las negociaciones;

   d) en relación con los acuerdos o arreglos con terceros Estados para su participación en operaciones de gestión de crisis de la PCSD a que se refiere el artículo 10, apartado 1, letra c), del anexo A, el SEAE asistirá al AR en las propuestas que se presenten al Consejo de conformidad con el artículo 218, apartados 3, 5 y 6, del TFUE, y apoyará al AR en las negociaciones.

3. Cuando los acuerdos de seguridad de la información estipulen que deben aprobarse acuerdos técnicos de aplicación entre la Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE y la autoridad de seguridad competente del tercer Estado u organización internacional de que se trate, tales acuerdos tendrán en cuenta el grado de protección aportado por la normativa, estructuras y procedimientos de seguridad existentes en dicho tercer Estado u organización internacional. La Dirección encargada de la seguridad de la sede y la seguridad de la información del SEAE se coordinará con la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad de la Comisión y con la Oficina de Seguridad de la Secretaría General del Consejo en lo que respecta a dichas disposiciones.

4. Cuando el SEAE necesite intercambiar durante largo tiempo información clasificada de un grado no superior a «RESTREINT UE/EU RESTRICTED» con un tercer Estado o una organización internacional y se haya determinado que la otra parte no cuenta con un sistema de seguridad suficientemente desarrollado como para celebrar un acuerdo de seguridad de la información, el AR podrá, previo dictamen favorable y unánime del Comité de Seguridad del SEAE de acuerdo con el artículo 15, apartado 5, de la presente Decisión, celebrar un acuerdo administrativo con las autoridades de seguridad competentes del tercer Estado o la organización internacional.

5. No se intercambiará ICUE por medios electrónicos con un tercer Estado u organización internacional a menos que así se estipule de forma explícita en el acuerdo de seguridad de la información o en el acuerdo administrativo.

6. En el marco de un acuerdo administrativo de intercambio de información clasificada, tanto el SEAE como el tercer Estado u organización internacional designarán un registro como principal punto de entrada y salida de la información clasificada que se intercambie. En el caso del SEAE, será el registro central.

7. Por regla general, los acuerdos administrativos adoptarán la forma de un canje de notas.

III VISITAS DE EVALUACIÓN

8. Las visitas de evaluación contempladas en el artículo 17 de la presente Decisión se realizarán de mutuo acuerdo con el tercer Estado u organización internacional de que se trate, y en ellas se valorarán:

   a) el marco regulador aplicable para proteger la información clasificada;

   b) cualesquiera características específicas de las leyes, reglamentos, políticas o procedimientos en materia de seguridad del tercer Estado u organización internacional que puedan incidir en el grado máximo de información clasificada que puede intercambiarse;

   c) las medidas y procedimientos de seguridad establecidos para la protección de la información clasificada; y

   d) los procedimientos de habilitación de seguridad del grado correspondiente al de la ICUE que ha de cederse.

9. No se intercambiará ICUE sin que previamente se haya realizado una visita de evaluación y se haya determinado el grado de la información clasificada que puede intercambiarse entre las partes habida cuenta de la equivalencia del grado de protección que se le brinde.

   Si, durante una visita de evaluación, el AR tiene conocimiento de razones excepcionales o urgentes para intercambiar información clasificada, la Autoridad de Seguridad del SEAE:

   a) recabará el consentimiento previo por escrito del originador para confirmar que no haya objeciones a la cesión; y

   b) podrá acordar la cesión, siempre que haya obtenido el dictamen favorable y unánime de los Estados miembros representados en el Comité de Seguridad del SEAE.

   Si el SEAE no puede determinar el originador, la Autoridad de Seguridad del SEAE asumirá la responsabilidad de aquel tras obtener el dictamen favorable y unánime del Comité de Seguridad del SEAE.

IV. AUTORIDAD PARA CEDER ICUE A TERCEROS ESTADOS U ORGANIZACIONES INTERNACIONALES

10. Cuando exista un marco para el intercambio de información clasificada con un tercer Estado u organización internacional, de conformidad con el artículo 10, apartado 1, del anexo A, la decisión de cesión de ICUE por parte del SEAE a un tercer Estado u organización internacional será adoptada por la Autoridad de Seguridad del SEAE.

11. Cuando el originador de la información clasificada que vaya a cederse, incluidos los originadores del material fuente que contenga, no sea el SEAE, la Autoridad de Seguridad del SEAE deberá recabar primero el consentimiento escrito del originador para confirmar que no haya objeciones a la cesión. Si el SEAE no puede determinar el originador, la Autoridad de Seguridad del SEAE asumirá la responsabilidad de aquel tras obtener el dictamen favorable unánime de los Estados miembros representados en el Comité de Seguridad del SEAE.

V. CESIÓN *AD HOC* CON CARÁCTER EXCEPCIONAL DE ICUE

12. A falta de uno de los marcos indicados en el artículo 10, apartado 1, del anexo A y cuando los intereses de la UE o de uno o más de sus Estados miembros requieran la cesión de ICUE por razones políticas, operativas o urgentes, podrá cederse ICUE con carácter excepcional a un tercer Estado u organización internacional una vez adoptadas las medidas que se indican a continuación.

   La Autoridad de Seguridad del SEAE encargada de la seguridad, tras verificar que se reúnan las condiciones indicadas en el apartado 11 anterior:

   a) comprobará, en la medida de lo posible y en colaboración con las autoridades de seguridad del tercer Estado u organización internacional de que se trate, que la normativa, estructuras y procedimientos de seguridad de estos garantizan que la ICUE que se les ceda será protegida con arreglo a normas no menos estrictas que las establecidas por la presente Decisión;

b) invitará al Comité de Seguridad del SEAE a emitir, basándose en la información disponible, un dictamen sobre el grado de confianza que deba concederse a la normativa, estructuras y procedimientos de seguridad del tercer Estado u organización internacional al que se vaya a cederse a la ICUE; y

c) podrá acordar la cesión, siempre que haya obtenido el dictamen favorable y unánime de los Estados miembros representados en el Comité de Seguridad del SEAE.

13. A falta de uno de los marcos indicados en el artículo 10, apartado 1, del anexo A, la tercera parte en cuestión se comprometerá por escrito a proteger debidamente la ICUE.

Apéndice A

DEFINICIONES

A los efectos de la presente Decisión, se entenderá por:

a) «Acreditación»: el proceso que concluye con la declaración formal de la Autoridad de Acreditación de Seguridad (AAS) de que un sistema ha recibido la correspondiente aprobación para tratar material de un grado determinado de clasificación en un modo específico de seguridad en su entorno operativo y con un nivel aceptable de riesgo, en el entendimiento de que se aplica un conjunto aprobado de medidas de seguridad técnicas, físicas, organizativas y procedimentales.

b) «Activos»: todo lo que tenga valor para una organización, para su funcionamiento y continuidad, incluidos los recursos de información disponibles para llevar a cabo su misión.

c) «Autorización para acceder a ICUE»: una autorización de la Autoridad de Seguridad del SEAE concedida de conformidad con la presente Decisión previa emisión de una HPS por las autoridades competentes de un Estado miembro y que acredite que una persona puede tener acceso a ICUE de un determinado grado («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información —con arreglo al artículo 2 del anexo A I.

d) «Fallo en la seguridad»: una acción u omisión de una persona que sea contraria a las normas de seguridad establecidas en la presente Decisión o a las políticas o directrices de seguridad que recojan las medidas necesarias para su aplicación.

e) «Ciclo de vida de un SIC»: la duración completa de la existencia de un SIC, que comprende inicio, concepción, planificación, análisis de requisitos, diseño, desarrollo, pruebas, aplicación, funcionamiento, mantenimiento y desmantelamiento.

f) «Contrato clasificado»: el contrato celebrado entre el SEAE y un contratista para el suministro de bienes, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique el acceso a ICUE o la creación de ICUE.

g) «Subcontrato clasificado»: el contrato celebrado por un contratista del SEAE con otro contratista (denominado «subcontratista») para el suministro de bienes, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique el acceso a ICUE o la creación de ICUE.

h) «Sistema de información y comunicaciones» (SIC): el sistema que permite manejar información en formato electrónico. Un sistema de información y comunicaciones abarca todos los activos necesarios para su funcionamiento, incluidos la infraestructura, la organización y los recursos de personal e información.

i) «Comprometimiento de la ICUE»: la revelación total o parcial de ICUE a personas o entidades no autorizadas —véase el artículo 9, apartado 2.

j) «Contratista»: la persona física o jurídica con capacidad legal para celebrar contratos.

k) «Productos criptográficos»: algoritmos criptográficos, módulos criptográficos de hardware y software, y productos que incluyan detalles de aplicación, documentación asociada y claves.

l) «Operación PCSD»: una operación militar o civil de gestión de crisis en virtud del título V, capítulo 2, del TUE.

m) «Desclasificación»: supresión de toda clasificación de seguridad.

n) «Defensa en profundidad»: la aplicación de una serie de medidas de seguridad organizadas a modo de barreras sucesivas de defensa.

o) «Autoridad de Seguridad Designada» (ASD): una autoridad responsable ante la Autoridad Nacional de Seguridad (ANS) de un Estado miembro, encargada de comunicar a sociedades industriales o de otra índole la política nacional sobre todos los aspectos de la seguridad industrial y de facilitarles dirección y asistencia para su aplicación. La función de ASD podrá ser ejercida por la ANS o por cualquier otra autoridad competente.

p) «Documento»: toda información registrada, independientemente de su soporte o características físicas.

q) «Reducción del grado de clasificación»: reducción del grado de clasificación de seguridad.

r) «Información clasificada de la UE» (ICUE): toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios de sus Estados miembros —véase el artículo 2, letra f).

s) «Habilitación de seguridad de establecimiento»: la certificación administrativa por parte de una ANS o una ASD de que, desde el punto de vista de la seguridad, un determinado establecimiento puede brindar un nivel adecuado de protección a la ICUE de un grado específico de clasificación de seguridad, y de que el personal que trabaja en dicho establecimiento y necesita acceder a ICUE ha sido debidamente habilitado y ha sido instruido sobre los requisitos de seguridad necesarios para acceder a la ICUE y para protegerla.

t) «Manejo» de ICUE: toda intervención posible a la que pueda estar sujeta a lo largo de su ciclo de vida la ICUE, es decir: producción, tratamiento, traslado, reducción del nivel de clasificación, desclasificación y destrucción. En relación con los SIC abarca asimismo su recopilación, exposición, transmisión y almacenamiento.

u) «Poseedor»: persona debidamente autorizada con una probada necesidad de conocer la información, que está en posesión de cualquier ICUE y es, por tanto, responsable de su protección.

v) «Sociedad industrial u otro tipo de entidad»: una entidad que participa en el suministro de bienes, la ejecución de obras o la prestación de servicios. Puede tratarse de sociedades industriales, comerciales y de servicios o de centros científicos, de investigación, educativos y de desarrollo, o de individuos que trabajen por cuenta propia.

w) «Seguridad industrial»: la aplicación de medidas encaminadas a garantizar la protección de la ICUE por los contratistas o subcontratistas durante las negociaciones precontractuales y durante toda la vigencia de los contratos clasificados —véase el artículo 9, apartado 1, del anexo A.

x) «Garantía de la información» (GI): en el ámbito de los sistemas de información y comunicaciones, la confianza en que esos sistemas protejan la información que manejan y funcionen como es necesario que lo hagan, cuando así se precise, bajo el control de sus usuarios legítimos. Una GI efectiva ha de asegurar unos niveles apropiados de confidencialidad, integridad, disponibilidad, no repudio y autenticidad. La GI se basará en un proceso de gestión del riesgo —véase el artículo 8, apartado 1, del anexo A.

y) «Interconexión»: a efectos de la presente Decisión, la conexión directa entre dos o más sistemas informáticos para compartir datos y otros recursos de información (por ejemplo, comunicación) de forma unidireccional o multidireccional —véase el anexo A IV, apartado 31.

z) «Tratamiento de la información clasificada»: la aplicación de medidas administrativas de control de la ICUE a lo largo de todo su ciclo de vida que completen las medidas contempladas en los artículos 5, 6 y 8 y contribuyan, así, a disuadir, descubrir y subsanar cualquier acto deliberado o accidental que pueda suponer la pérdida o compromiso de dicha información. Estas medidas se refieren, en particular, a la producción, registro, copia, traducción, traslado, manejo, almacenamiento y destrucción de ICUE —véase el artículo 7, apartado 1, del anexo A.

aa) «Material»: todo documento, máquina o aparato, producido o en proceso de producción.

bb) «Originador»: la institución, agencia u organismo de la UE, del Estado miembro, del tercer Estado o de la organización internacional bajo cuya autoridad se haya producido información clasificada o se haya introducido en las estructuras de la UE.

cc) «Seguridad en el personal»: la aplicación de medidas que garanticen que el acceso a la ICUE se conceda únicamente a personas que:

— tengan necesidad de conocerla;

— hayan sido habilitadas para el grado de clasificación correspondiente para acceder a información de grado «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior, o bien hayan sido debidamente autorizadas en virtud de sus funciones con arreglo a las leyes y reglamentos nacionales; y

— hayan sido instruidas sobre sus responsabilidades

con arreglo al artículo 5, apartado 1, del anexo A;

dd) «Habilitación personal de seguridad» (HPS) para acceder a ICUE: la declaración de una autoridad competente de un Estado miembro, efectuada al término de una investigación de seguridad realizada por las autoridades competentes del Estado miembro, mediante la cual se acredita que una persona puede tener acceso a ICUE de un determinado grado («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información; de la persona que se ajuste a esta descripción se dirá que está «habilitada».

ee) «Certificado de habilitación personal de seguridad» (CHPS): el certificado expedido por una autoridad competente que acredite que una persona está habilitada y dispone de una HPS válida o de una autorización del Director de la seguridad de la sede y la seguridad de la información del SEAE para acceder a ICUE, y que indique el grado de ICUE al que puede tener acceso («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior), el período de validez de la HPS y la fecha de caducidad del propio certificado.

ff) «Seguridad física»: la aplicación de medidas de protección física y técnica para impedir el acceso no autorizado a ICUE —véase el artículo 6 del anexo A.

gg) «Instrucciones de seguridad de un programa o proyecto»: lista de procedimientos de seguridad aplicables a un programa o proyecto específico para tipificar los procedimientos de seguridad. Puede ser objeto de revisión a lo largo de la ejecución del programa o proyecto.

hh) «Registro»: la aplicación de procedimientos para registrar el ciclo de vida de la información, incluida su divulgación y destrucción —véase el anexo A III, apartado 21.

ii) «Riesgo residual»: el riesgo que persiste una vez aplicadas las medidas de seguridad, dado que no es posible contrarrestar todas las amenazas ni eliminar todas las vulnerabilidades.

jj) «Riesgo»: la posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades internas o externas de una organización o de alguno de los sistemas que esta utilice y al hacerlo ocasione daños a la organización o a sus activos tangibles o intangibles. Se mide como la combinación de la probabilidad de que se cumplan las amenazas y de su repercusión.

kk) «Aceptación del riesgo»: la decisión de aceptar, una vez tratado el riesgo, la persistencia de un riesgo residual.

ll) «Evaluación del riesgo»: la determinación de las amenazas y las vulnerabilidades, y la realización del correspondiente análisis del riesgo, es decir, el análisis de la probabilidad y de las repercusiones.

mm) «Comunicación del riesgo»: la concienciación sobre los riesgos a las comunidades de usuarios de SIC, y la información de tales riesgos a las autoridades responsables de la aprobación y a las autoridades operativas.

nn) «Proceso de gestión del riesgo de seguridad»: la totalidad del proceso de determinación, control y disminución de acontecimientos inciertos que puedan afectar a la seguridad de una organización o de alguno de los sistemas que esta utilice. Abarca todas las actividades relacionadas con los riesgos, incluida la evaluación, tratamiento, aceptación y comunicación.

oo) «Tratamiento del riesgo»: la atenuación, supresión o reducción del riesgo (adoptando una combinación adecuada de medidas técnicas, físicas, de gestión o de procedimiento), transferencia del riesgo o seguimiento de este.

pp) «Cláusula sobre aspectos de la seguridad»: el conjunto de condiciones contractuales especiales impuestas por la autoridad contratante, que forman parte integrante de un contrato clasificado que conlleve el acceso a ICUE o la creación de ICUE y que enumeran los requisitos de seguridad o los elementos del contrato que requieren protección de seguridad —véase el anexo A V, sección II.

qq) «Guía de clasificación de seguridad»: el documento que describe los elementos de un programa o contrato que están clasificados, con especificación de los grados de clasificación de seguridad aplicables. La guía de clasificación de seguridad podrá ampliarse durante toda la vigencia del programa o contrato, y se podrá reducir el grado de clasificación o reclasificar los elementos de información; cuando exista una guía de clasificación de seguridad, formará parte de la cláusula sobre aspectos de la seguridad —véase el anexo A V, sección II.

rr) «Investigación de seguridad»: el procedimiento de investigación efectuado por la autoridad competente de un Estado miembro con arreglo a las disposiciones legales y reglamentarias nacionales, con el fin de obtener la garantía de que no se conocen datos desfavorables que impidan conceder a una persona determinada una HPS nacional o de la UE para acceder a ICUE de un determinado grado («CONFIDENTIEL UE/EU CONFIDENTIAL» o superior).

ss) «Procedimientos operativos de seguridad»: una descripción de cómo debe aplicarse la política de seguridad, de los procedimientos operativos que deben seguirse y de las responsabilidades del personal.

tt) «Información delicada no clasificada»: la información o material que el SEAE debe proteger por razón de obligaciones legales establecidas en los Tratados o en actos adoptados en aplicación de este, o por razón de su carácter delicado. La información delicada no clasificada incluye, pero no se limita a, la información o el material cubiertos por la obligación de secreto profesional, en virtud de lo dispuesto en el artículo 339 del TFUE; la información cubierta por los intereses protegidos en el artículo 4 del Reglamento (CE) n.º 1049/2001 ([1]), leído en relación con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea; o los datos personales incluidos en el ámbito de aplicación del Reglamento (UE) 2018/1725.

uu) «Declaración de requisitos específicos de seguridad»: un conjunto de principios vinculantes y requisitos detallados de seguridad que son de observancia y aplicación obligatorias y cimientan el proceso de certificación y acreditación de los SIC.

vv) «TEMPEST»: la investigación, el estudio y el control de las emanaciones electromagnéticas comprometedoras y las medidas para suprimirlas.

ww) «Amenaza»: la posible causa de un incidente no deseado que pueda ocasionar daños a una organización o a alguno de los sistemas que esta utilice; las amenazas pueden ser accidentales o deliberadas (maliciosas) y constan de elementos amenazadores, posibles blancos y métodos de ataque.

xx) «Vulnerabilidad»: una debilidad, cualquiera que sea su naturaleza, que pueda ser aprovechada por una o varias amenazas. La vulnerabilidad puede ser resultado de una omisión o guardar relación con una deficiencia en el grado, completitud o coherencia de los controles, y puede ser técnica, física, procedimental, organizativa u operativa.

([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).

Apéndice B

Correspondencia de las clasificaciones de seguridad

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/UE CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Bélgica	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Nota ([1]) a continuación
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
República Checa	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dinamarca	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG| à
Alemania	STRENG GEHEIM	GEHEIM	VS ([2]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abrev.: ΑΑΠ	Απόρρητο Abrev.: (ΑΠ)	Εμπιστευτικό Abrev.: (ΕΜ)	Περιορισμένης Χρήσης Abrev.: (ΠΧ)
España	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francia	TRÈS SECRET TRÈS SECRET DÉFENSE ([3])	SECRET SECRET DÉFENSE ([3])	CONFIDENTIEL DÉFENSE ([3]) ([4])	Nota ([5]) a continuación
Croacia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Chipre	Άκρως Απόρρητο Abrev.: (ΑΑΠ)	Απόρρητο Abrev.: (ΑΠ)	Εμπιστευτικό Abrev.: (ΕΜ)	Περιορισμένης Χρήσης Abrev.: (ΠΧ)
Letonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungría	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»

Malta	L-Oġħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([6])
Países Bajos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Rumanía	Strict secret de importanță deosebită	Strict secret	Secret	Secreto de serviciu
Eslovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Eslovaquia	Přísně tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLI-NEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suecia	Kvaliciferat hemlig	Hemlig	Konfidentiell	Begränsat hemlig

([1]) «Diffusion restreinte/Beperkte Verspreiding» no constituye una clasificación de seguridad en Bélgica. Bélgica maneja y protege la información «RESTREINT UE/EU RESTRICTED» con un rigor no inferior al de las reglas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

([2]) Alemania: VS = Verschlusssache.

([3]) La información generada por Francia antes del 1 de julio de 2021 con clasificación «TRÈS SECRET DÉFENSE», «SECRET DÉFENSE» y «CONFIDENTIEL DÉFENSE» sigue manejándose y protegiéndose en el grado equivalente a «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET» y «CONFIDENTIEL UE/EU CONFIDENTIAL», respectivamente.

([4]) Francia trata y protege la información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL» con arreglo a las medidas de protección de seguridad para la información «SECRET».

([5]) Francia no utiliza la clasificación «RESTREINT» en su sistema nacional. Francia maneja y protege la información «RESTREINT UE/EU RESTRICTED» con un rigor no inferior al de las reglas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

([6]) En Malta, las marcas en maltés e inglés pueden utilizarse indistintamente.