Este documento es un instrumento de documentación y no compromete la responsabilidad de las instituciones

►**B**

DECISIÓN DEL CONSEJO

de 23 de septiembre de 2013

sobre las normas de seguridad para la protección de la información clasificada de la UE

(2013/488/UE)

(DO L 274 de 15.10.2013, p. 1)

Modificado por:

		Diario Oficial		
		n°	página	fecha
►**M1**	Decisión 2014/233/UE del Consejo de 14 de abril de 2014	L 125	72	26.4.2014

▼B

DECISIÓN DEL CONSEJO

de 23 de septiembre de 2013

sobre las normas de seguridad para la protección de la información clasificada de la UE

(2013/488/UE)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 240, apartado 3,

Vista la Decisión 2009/937/UE del Consejo, de 1 de diciembre de 2009, por la que se aprueba su Reglamento interno [1], y, en particular, su artículo 24,

Considerando lo siguiente:

(1) A fin de desempeñar las actividades del Consejo en todos aquellos ámbitos en los que es necesario manejar información clasificada, es conveniente establecer un sistema integral de seguridad para la protección de la información clasificada aplicable al Consejo, a su Secretaría General y a los Estados miembros.

(2) La presente Decisión debe aplicarse siempre que el Consejo, sus órganos preparatorios y la Secretaría General del Consejo (SGC) manejen información clasificada de la UE (ICUE).

(3) De conformidad con sus disposiciones legales y reglamentarias nacionales y en la medida de lo necesario para el funcionamiento del Consejo, los Estados miembros deben respetar la presente Decisión siempre que sus autoridades competentes, personal o contratistas manejen ICUE, a fin de que todos ellos puedan tener la seguridad de que se garantiza un nivel equivalente de protección a dicha información.

(4) El Consejo, la Comisión y el Servicio Europeo de Acción Exterior (SEAE) se han comprometido a aplicar estándares de seguridad equivalentes para la protección de la ICUE.

(5) El Consejo subraya la importancia de que el Parlamento Europeo y las demás instituciones, órganos, organismos o agencias de la Unión queden asociados, cuando proceda, a los principios, estándares y normas de protección de la información clasificada que resultan necesarios para proteger los intereses de la Unión y de sus Estados miembros.

(6) El Consejo debe establecer el marco adecuado para compartir ICUE que obre en su poder con otras instituciones, órganos, organismos o agencias de la Unión, según proceda, de conformidad con la presente Decisión y acuerdos interinstitucionales vigentes.

(7) Los órganos y las agencias de la UE creados en virtud del título V, capítulo 2, del Tratado de la Unión Europea (TUE), Europol y Eurojust deben aplicar, en el contexto de su organización interna, los principios básicos y los estándares mínimos para la protección de la ICUE establecidos en la presente Decisión, cuando así lo disponga el acto en virtud del cual se hayan creado.

[1] DO L 325 de 11.12.2009, p. 35.

▼B

(8) Las operaciones de gestión de crisis establecidas al amparo del título V, capítulo 2, del TUE y su personal deben aplicar las normas de seguridad adoptadas por el Consejo para la protección de la ICUE cuando así lo disponga el acto del Consejo al amparo del cual se hayan establecido.

(9) Los representantes especiales de la UE y los miembros de sus equipos deben aplicar las normas de seguridad adoptadas por el Consejo para la protección de la ICUE cuando así lo disponga el acto pertinente del Consejo.

(10) La presente Decisión se adopta 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.

(11) La presente Decisión se adopta sin perjuicio de las prácticas vigentes en los Estados miembros respecto de la información que proporcionen a sus Parlamentos nacionales sobre las actividades de la Unión.

(12) A fin de garantizar que las normas de seguridad para la protección de la ICUE se apliquen oportunamente en lo que atañe a la adhesión de la República de Croacia a la Unión Europea, la presente Decisión debe entrar en vigor el día de su publicación.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Objeto, ámbito de aplicación y definiciones

1. La presente Decisión establece los principios básicos y los estándares mínimos de seguridad para la protección de la Información clasificada de la Unión Europea (ICUE).

2. Dichos principios básicos y estándares mínimos se aplicarán al Consejo y a la SGC y deberán ser respetados por los Estados miembros, de conformidad con sus respectivas disposiciones legales y reglamentarias nacionales, a fin de que todos ellos puedan tener la seguridad de que se garantiza un nivel equivalente de protección a la ICUE.

3. A los efectos de la presente Decisión, se aplicarán las definiciones que figuran en el apéndice A.

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 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 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 Estados miembros;

▼B

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 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 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. Las autoridades competentes se asegurarán 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. El Consejo aprobará una política 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 de la Unión información clasificada que lleve una marca nacional de clasificación de seguridad, el Consejo y la SGC protegerán 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.

4. Un agregado de ICUE podrá justificar un grado de protección que corresponda a una clasificación más elevada que la asignada a cada uno de sus componentes.

▼B

Artículo 5

Gestión del riesgo de seguridad

1. La gestión de los riesgos que corre la ICUE adoptará la forma de un proceso, el cual tendrá por objetivo determinar los riesgos de seguridad conocidos, definir las medidas de seguridad para reducir dichos riesgos a un nivel aceptable, de conformidad con los principios básicos y los estándares mínimos establecidos en la presente Decisión, y adecuar esas medidas al concepto de defensa en profundidad definido en el apéndice A. La eficacia de dichas medidas será continuamente evaluada.

2. Las medidas de seguridad para proteger la ICUE a lo largo de todo su ciclo de vida serán acordes, en particular, con su clasificación de seguridad, la forma y el volumen de la información o material, la ubicación y construcción de la instalación en el que se conserve, y la amenaza de actividades maliciosas o delictivas, evaluadas localmente, en particular el espionaje, el sabotaje y el terrorismo.

3. Los planes de contingencia tendrán en cuenta la necesidad de proteger la ICUE en situaciones de emergencia, con el fin de impedir el acceso o la revelación no autorizados y la pérdida de integridad o disponibilidad.

4. En los planes de continuidad de la actividad se incluirán medidas preventivas y de recuperación para reducir al máximo las repercusiones de fallos o incidentes graves en el manejo y almacenamiento de ICUE.

Artículo 6

Aplicación de la presente Decisión

1. En caso necesario, el Consejo, previa recomendación del Comité de Seguridad, aprobará políticas de seguridad que establezcan medidas de aplicación de la presente Decisión.

2. El Comité de Seguridad podrá acordar, dentro de su ámbito de competencias, directrices de seguridad que completen o faciliten la aplicación de la presente Decisión y de las políticas de seguridad aprobadas por el Consejo.

Artículo 7

Seguridad en el personal

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 conocer,

— hayan sido habilitadas para el grado de clasificación correspondiente, en caso necesario, y

— hayan sido instruidas sobre sus responsabilidades.

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

▼B

3. Todas las personas de la SGC cuyas funciones puedan requerir el acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, o su manejo, deberán haber sido habilitadas para el grado correspondiente antes de poder acceder a dicha información. Estas personas deberán ser autorizadas por la autoridad facultada para proceder a los nombramientos de la SGC para acceder a ICUE de un determinado nivel y hasta una fecha determinada.

4. El personal de los Estados miembros a que se refiere el artículo 15, apartado 3, cuyas funciones puedan requerir el acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior deberá haber sido habilitado para el grado correspondiente o haber sido debidamente autorizado en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales, antes de poder acceder a dicha información.

5. 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 dichas responsabilidades.

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

Artículo 8

Seguridad física

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 segregar al 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 artículo 10, apartado 2.

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 II, y serán aprobadas por la autoridad de seguridad competente.

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

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

▼B

Artículo 9

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 7, 8 y 10 y contribuyan, así, a disuadir y descubrir cualquier acto deliberado o accidental que pueda comprometer o suponer la pérdida de dicha información. Estas medidas se refieren, en particular, a la producción, registro, copia, traducción, reducción del grado de clasificación, desclasificación, traslado 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 de la SGC y de los Estados miembros 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 competente.

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 criptológicos aprobados de conformidad con lo dispuesto en el artículo 10, apartado 6;

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 criptológicos aprobados de conformidad con lo dispuesto en el artículo 10, apartado 6, o

   ii) en todos los demás casos, según las prescripciones de la autoridad de seguridad competente y de acuerdo con las pertinentes medidas de protección establecidas en el anexo III.

5. Las disposiciones de aplicación del presente artículo figuran en los anexos III y IV.

Artículo 10

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.

▼B

2. Por «sistema de información y comunicaciones» (SIC) se entenderá el sistema que permite manejar información en formato electrónico. Un SIC abarca todos los medios necesarios para su funcionamiento, incluidos la infraestructura, la organización y los recursos de personal e información. La presente Decisión se aplicará a los SIC que manejen ICUE.

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

4. Todos los SIC 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.

5. Se aplicarán medidas de seguridad a fin de proteger los SIC que manejen información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior de modo que dicha información no pueda verse comprometida como consecuencia de emanaciones electromagnéticas no intencionadas («medidas de seguridad TEMPEST»). Estas medidas de seguridad serán proporcionadas al riesgo de explotación de la información y al grado de clasificación de esta.

6. Cuando la protección de la ICUE se realice mediante productos criptológicos, dichos productos se aprobarán del siguiente modo:

a) la confidencialidad de la información clasificada de grado SECRET UE/EU SECRET o superior deberá protegerse mediante productos criptológicos aprobados por el Consejo, en su calidad de Autoridad de Certificación Criptológica (ACC), por recomendación del Comité de Seguridad;

b) la confidencialidad de la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o RESTREINT UE/EU RESTRICTED deberá protegerse mediante productos criptológicos aprobados por el Secretario General del Consejo («Secretario General»), en su calidad de ACC, por recomendación del Comité de Seguridad.

No obstante lo dispuesto en la letra b), dentro de los sistemas nacionales de los Estados miembros, la confidencialidad de la ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o RESTREINT UE/EU RESTRICTED podrá protegerse mediante productos criptológicos aprobados por la ACC de un Estado miembro.

7. 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 IV.

▼B

8. Las autoridades competentes de la SGC y de los Estados miembros designarán, respectivamente, 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).

9. Para cada sistema, las autoridades competentes de la SGC y de los Estados miembros, respectivamente, designarán:

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

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

10. Las disposiciones de aplicación del presente artículo figuran en el anexo IV.

Artículo 11

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. Estos contratos no podrán suponer el acceso a información clasificada de grado TRÈS SECRET UE/EU TOP SECRET.

2. La SGC 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 o un acuerdo administrativo de conformidad con el artículo 13, apartado 2, letras a) o b), el desempeño de funciones que conlleven el acceso a ICUE o su manejo o almacenamiento.

3. Cuando actúe como órgano de contratación, la SGC 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.

4. La Autoridad Nacional de Seguridad (ANS), la Autoridad de Seguridad Designada (ASD) o cualquier otra autoridad competente de cada Estado miembro velará por que, en la medida en que las disposiciones legales y reglamentarias nacionales lo permitan, los contratistas y subcontratistas registrados en su territorio tomen todas las medidas adecuadas para proteger la ICUE durantes las negociaciones precontractuales y durante la ejecución de un contrato clasificado.

5. La ANS, la ASD o cualquier otra autoridad de seguridad competente de cada Estado miembro velará por que, de conformidad con las disposiciones legales y reglamentarias nacionales, los contratistas y subcontratistas registrados en el respectivo Estado miembro que participen en contratos o subcontratos clasificados que requieran el acceso a 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, estén en posesión de una habilitación de seguridad de establecimiento del grado de clasificación requerido.

▼B

6. La ANS, la ASD o cualquier otra autoridad de seguridad competente que corresponda concederá una habilitación personal de seguridad (HPS), de conformidad con las disposiciones legales y reglamentarias nacionales y las normas mínimas de seguridad establecidas en el anexo I, al 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.

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

Artículo 12

Compartir la ICUE

1. El Consejo establecerá las condiciones en las que podrá compartir ICUE que obre en su poder con otras instituciones, órganos, organismos o agencias de la Unión. Podrá crearse un marco adecuado para ello, incluido mediante la celebración de acuerdos interinstitucionales u otros acuerdos, cuando sea necesario para tal fin.

2. 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 13

Intercambio de información clasificada con terceros Estados y organizaciones internacionales

1. Cuando el Consejo determine que existe la necesidad de intercambiar ICUE con un tercer Estado o una organización internacional, se establecerá un marco adecuado para ello.

2. Con el fin de establecer dicho marco y definir normas de protección recíproca de la información clasificada que se intercambie:

a) la Unión celebrará con terceros Estados u organizaciones internacionales acuerdos sobre procedimientos de seguridad para la protección e intercambio de información clasificada («acuerdos para la seguridad de la información»), o

b) el Secretario General podrá celebrar en nombre de la SGC acuerdos administrativos a tal efecto de conformidad con el punto 17 del anexo VI, si la ICUE que ha de comunicarse no supera, por lo general, el grado de clasificación RESTREINT UE/EU RESTRICTED.

3. Los acuerdos de seguridad de la información o los acuerdos administrativos a que se refiere el apartado 2 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.

▼B

4. La decisión de ceder ICUE producida en el Consejo a un tercer Estado u organización internacional será adoptada por el Consejo, 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 Unión. Si el originador de la información clasificada que se desea ceder no es el Consejo, la SGC deberá recabar el consentimiento previo por escrito del originador antes de comunicarla. En caso de que no sea posible determinar el originador, el Consejo asumirá la responsabilidad de aquel.

5. Se organizarán visitas de evaluación, a fin de verificar la eficacia de las medidas de seguridad establecidas en el tercer país o en la organización internacional de que se trate para proteger la ICUE proporcionada o intercambiada.

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

Artículo 14

Fallos de seguridad y comprometimiento de la ICUE

1. Un fallo de seguridad se produce como resultado de una acción u omisión de una persona contraria a las normas de seguridad establecidas en la presente Decisión.

2. Se produce un comprometimiento de la ICUE cuando, como consecuencia de un fallo de seguridad, dicha información se pone total o parcialmente en conocimiento de personas no autorizadas.

3. Todo fallo o posible fallo de seguridad deberá comunicarse inmediatamente a la autoridad de seguridad competente.

4. Cuando se tenga conocimiento o sospechas fundadas de que una ICUE se ha visto comprometida o se ha perdido, la ANS u otra autoridad competente tomará todas las medidas oportunas, de conformidad con las disposiciones legales y reglamentarias pertinentes, para:

a) informar al originador de la información;

b) asegurarse de que el personal que investiga el caso con el fin de esclarecer los hechos no esté directamente implicado en el fallo de seguridad;

c) evaluar el posible perjuicio causado a los intereses de la Unión o de los Estados miembros;

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

e) notificar a las autoridades que corresponda las medidas adoptadas.

5. La persona que sea responsable de un fallo de las normas de seguridad establecidas en la presente Decisión podrá ser objeto de medidas disciplinarias de conformidad con la normativa aplicable. La persona que sea responsable de un comprometimiento o pérdida de ICUE podrá ser objeto de medidas disciplinarias o de una acción judicial de conformidad con las disposiciones legales y reglamentarias aplicables.

▼B

Artículo 15

Responsabilidad de la aplicación

1. El Consejo tomará todas las medidas necesarias para garantizar la coherencia general de la aplicación de la presente Decisión.

2. El Secretario General tomará todas las medidas necesarias para garantizar que, cuando manejen o almacenen ICUE o cualquier otra clase de información clasificada, tanto los funcionarios y otros agentes de la SGC como el personal destinado en comisión de servicio en la SGC y los contratistas externos de esta apliquen la presente Decisión en los locales empleados por el Consejo y dentro de la SGC.

3. Los Estados miembros adoptarán, de conformidad con sus disposiciones legales y reglamentarias nacionales, todas las medidas adecuadas para garantizar que, cuando se maneje o almacene ICUE, se respete la presente Decisión por:

a) el personal de las Representaciones Permanentes de los Estados miembros ante la Unión Europea y por los miembros de las Delegaciones nacionales que asistan a reuniones del Consejo o de sus órganos preparatorios o que participen en otras actividades del Consejo;

b) el resto del personal de las administraciones nacionales de los Estados miembros, incluido el personal destinado en ellas en comisión de servicio, con independencia de que ejerzan sus funciones en el territorio de los Estados miembros o en el extranjero;

c) las demás personas de los Estados miembros que, por sus funciones, estén debidamente autorizadas para acceder a ICUE, y

d) los contratistas de los Estados miembros, tanto en el territorio de los Estados miembros como en el extranjero.

Artículo 16

Organización de la seguridad en el Consejo

1. En el marco de su función de garantizar la coherencia general en la aplicación de la presente Decisión, el Consejo aprobará:

a) los acuerdos a que se refiere el artículo 13, apartado 2, letra a);

b) las decisiones por las que se autorice o se dé consentimiento para la cesión de ICUE originada en el Consejo o que obre en su poder a terceros Estados y organizaciones internacionales, respetando el principio del consentimiento previo del originador;

c) un programa anual de visitas de evaluación, por recomendación del Comité de Seguridad, para realizar visitas destinadas a evaluar los servicios y locales de los Estados miembros, de los órganos, agencias y entidades de la Unión que apliquen la presente Decisión o sus principios, y para efectuar visitas de evaluación a terceros Estados y organizaciones internacionales, con el fin de verificar la eficacia de las medidas establecidas para proteger la ICUE, y

▼B

d) las políticas de seguridad a que se refiere el artículo 6, apartado 1.

2. El Secretario General será la autoridad de seguridad de la SGC. En calidad de tal, el Secretario General:

a) aplicará la política de seguridad del Consejo y la revisará regularmente;

b) establecerá una coordinación con las ANS de los Estados miembros para todas las cuestiones de seguridad relacionadas con la protección de información clasificada pertinente para las actividades del Consejo;

c) concederá a los funcionarios y otros agentes de la SGC y a los expertos nacionales destinados en la SGC en comisión de servicio autorización para acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, de conformidad con el artículo 7, apartado 3;

d) cuando proceda, ordenará que se investigue toda situación real o supuesta de comprometimiento o pérdida de información clasificada que haya estado en posesión del Consejo o que haya originado este, y pedirá a las autoridades de seguridad competentes que le ayuden en dichas investigaciones;

e) realizará inspecciones periódicas de las medidas de seguridad adoptadas para la protección de la información clasificada en las instalaciones de la SGC;

f) realizará visitas periódicas para evaluar las medidas de seguridad adoptadas para la protección de la ICUE en los órganos, agencias y entidades de la Unión que apliquen la presente Decisión o sus principios;

g) realizará, junto con las ANS interesadas y de acuerdo con ellas, evaluaciones periódicas de las medidas de seguridad adoptadas para la protección de la ICUE en los servicios e instalaciones de los Estados miembros;

h) se cerciorará de que las medidas de seguridad estén adecuadamente coordinadas con las autoridades competentes de los Estados miembros que sean responsables de la protección de la información clasificada y, según proceda, con terceros Estados u organizaciones internacionales, en particular en lo tocante a la naturaleza de las amenazas para la seguridad de la ICUE y a los medios para protegerse de ellas, y

i) celebrará los acuerdos administrativos a que se refiere el artículo 13, apartado 2, letra b).

La Oficina de Seguridad de la SGC se pondrá a disposición del Secretario General para prestarle ayuda en el ejercicio de sus funciones.

3. Para la aplicación de lo dispuesto en el artículo 15, apartado 3, los Estados miembros:

a) designarán una ANS relacionada en el apéndice C responsable de las medidas de seguridad para la protección de la ICUE, con el fin de garantizar que:

   i) la ICUE que esté en posesión de cualquier departamento, órgano u organismo nacional, de carácter público o privado, en el territorio nacional o en el extranjero, esté protegida de conformidad con la presente Decisión,

   ii) se inspeccione o evalúe periódicamente el cumplimiento de las medidas de seguridad establecidas para la protección de la ICUE,

▼B

iii) toda persona empleada en una administración nacional o por un contratista a la que se pueda conceder acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior haya sido debidamente habilitada o debidamente autorizada por otros medios en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales,

iv) se elaboren los programas de seguridad que se consideren necesarios para minimizar el riesgo de que la ICUE se vea comprometida o se pierda,

v) para todas las cuestiones de seguridad relacionadas con la protección de la ICUE, exista una coordinación con las demás autoridades nacionales competentes, incluidas aquellas a los que se refiere la presente Decisión, y

vi) se dé respuesta a las solicitudes adecuadas de habilitación de seguridad, en particular las remitidas por cualquiera de los órganos, agencias y entidades de la Unión, las operaciones establecidas en virtud del título V, capítulo 2, del TUE y los Representantes Especiales de la UE (REUE) y sus equipos que apliquen la presente Decisión o sus principios;

b) se asegurarán de que sus autoridades competentes informen y asesoren a sus respectivos Gobiernos y, a través de estos, al Consejo, acerca de la naturaleza de las amenazas que pesan sobre la seguridad de la ICUE y sobre los medios para protegerse de ellas.

Artículo 17

Comité de Seguridad

1. Por la presente se crea un Comité de Seguridad. Este Comité examinará y evaluará las cuestiones de seguridad incluidas en el ámbito de aplicación de la presente Decisión y hará recomendaciones al Consejo cuando proceda.

2. El Comité de Seguridad estará integrado por representantes de las ANS de los Estados miembros; asistirá a sus reuniones un representante de la Comisión y del EEAS. El Comité de Seguridad estará presidido por el Secretario General o por la persona en quien este delegue. Se reunirá siguiendo instrucciones del Consejo o a instancias del Secretario General o de una ANS.

Se podrá invitar a representantes de los órganos, agencias y entidades de la Unión que apliquen la presente Decisión o sus principios, a asistir a las reuniones cuando se debatan cuestiones que les afecten.

3. El Comité de Seguridad organizará sus actividades de manera que pueda formular recomendaciones sobre aspectos específicos de la seguridad. Creará una subsección de expertos en cuestiones relativas a la GI, así como otras subsecciones de expertos, si fuera necesario. Elaborará los mandatos para dichas subsecciones y recibirá los informes que estas realicen sobre sus actividades, entre los que podrán figurar, si se considera oportuno, recomendaciones para el Consejo.

▼B

Artículo 18

Sustitución de anteriores decisiones

1. La presente Decisión deroga y sustituye la Decisión 2011/292/UE del Consejo ([1]).

2. Toda la ICUE clasificada conforme a la Decisión 2001/264/CE del Consejo ([2]) y a la Decisión 2011/292/UE seguirá estando protegida de acuerdo con las disposiciones pertinentes de la presente Decisión.

Artículo 19

Entrada en vigor

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

([1]) Decisión 2011/292/UE del Consejo, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 141 de 27.5.2011, p. 17).

([2]) Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo (DO L 101 de 11.4.2001, p. 1).

▼B

ANEXOS

ANEXO I

Seguridad en el personal

ANEXO II

Seguridad física

ANEXO III

Tratamiento de la información clasificada

ANEXO IV

Protección de la ICUE manejada en los SIC

ANEXO V

Seguridad industrial

ANEXO VI

Intercambio de información clasificada con terceros Estados y organizaciones internacionales

▼B

ANEXO I

SEGURIDAD EN EL PERSONAL

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 7. Define los criterios que determinan 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.

II. CONCESIÓN DE ACCESO A ICUE

2. Solo se concederá acceso a información clasificada a aquella persona:

   a) cuya necesidad de conocer se haya determinado;

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

   c) en el caso de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior:

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

      — en el caso de los funcionarios y otros agentes de la SGC y los expertos nacionales destinados en la SGC en comisión de servicio, a quien la autoridad facultada para proceder a los nombramientos de la SGC haya autorizado a acceder a ICUE, de conformidad con lo dispuesto en los puntos 16 a 25, de un determinado nivel y hasta una fecha determinada.

3. Cada Estado miembro y la SGC determinarán los puestos que, dentro de sus respectivas administraciones, exigen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior y requieren por tanto una habilitación de seguridad de grado correspondiente.

III. REQUISITOS PARA OBTENER LA HABILITACIÓN PERSONAL DE SEGURIDAD

4. Una vez recibida una solicitud debidamente autorizada, corresponderá a las ANS u otras autoridades nacionales competentes asegurarse de que se realizan las investigaciones de seguridad sobre aquellos de sus nacionales que deban tener acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. Las investigaciones se ajustarán a las disposiciones legales y reglamentarias nacionales a efectos de expedir una HPS o de ofrecer una garantía de que se concederá a una persona autorización para acceder a ICUE, según proceda.

5. En caso de que la persona resida en el territorio de otro Estado miembro o en un tercer Estado, las autoridades nacionales competentes solicitarán la colaboración de la autoridad competente del Estado de residencia, de conformidad con las disposiciones legales y reglamentarias nacionales. Los Estados miembros se prestarán ayuda mutua para la realización de las investigaciones de seguridad, de conformidad con las disposiciones legales y reglamentarias nacionales.

6. Cuando lo permitan las disposiciones legales y reglamentarias nacionales, las ANS u otras autoridades nacionales competentes podrán realizar investigaciones sobre no nacionales que deban tener acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. Las investigaciones se ajustarán a las disposiciones legales y reglamentarias nacionales.

▼B

Criterios para las investigaciones de seguridad

7. La lealtad, honradez y fiabilidad de una persona a efectos de la obtención de una habilitación de seguridad para acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se determinarán mediante una investigación de seguridad. La autoridad nacional competente realizará una evaluación global basada en el resultado de la investigación de seguridad. Los criterios principales que se aplicarán a este efecto incluirán, en la medida en que lo permitan las disposiciones legales y reglamentarias nacionales, el estudio de si la persona:

a) ha cometido o intentado cometer, o ha conspirado para cometer o ha sido cómplice en la comisión de cualquier acto de espionaje, terrorismo, sabotaje, traición o sedición;

b) está o ha estado vinculado con espías, terroristas, saboteadores o personas sobre las que pese una sospecha razonable de pertenecer a esta categoría de personas, o con representantes de organizaciones o Estados extranjeros, incluidos los servicios de inteligencia extranjeros, que puedan suponer una amenaza para la seguridad de la Unión o de sus Estados miembros, salvo que dicha relación haya sido autorizada en cumplimiento de una misión oficial;

c) es o ha sido miembro de cualquier organización que persiga, por medios violentos, subversivos u otros medios ilegales, entre otros, el derrocamiento del Gobierno de un Estado miembro, la alteración del orden constitucional de un Estado miembro o el cambio de su forma de Gobierno o de la política de su Gobierno;

d) respalda o ha respaldado a cualquier organización que responda a lo descrito en la letra c), o está estrechamente vinculado a miembros de este tipo de organizaciones;

e) ha ocultado, deformado o falseado deliberadamente información importante, especialmente en el ámbito de la seguridad, o ha mentido deliberadamente al cumplimentar un cuestionario de seguridad en el personal o en el curso de una entrevista de seguridad;

f) ha sido condenado por uno o varios delitos;

g) tiene un historial de dependencia del alcohol, consumo de drogas ilícitas o consumo abusivo de drogas lícitas;

h) tiene o ha tenido alguna conducta que pueda hacerlo vulnerable al chantaje u otro tipo de presiones;

i) ha demostrado, de obra o de palabra, su falta de honradez, deslealtad, falta de fiabilidad o de probidad;

j) ha infringido de manera grave o reiterada las normas de seguridad, o ha intentado realizar o ha realizado actividades no autorizadas en relación con sistemas de información y comunicaciones, y

k) puede verse sujeto a presiones (por ejemplo, por tener la nacionalidad de uno o varios países no pertenecientes a la UE o a través de familiares o allegados que puedan ser vulnerables frente a servicios de inteligencia extranjeros, grupos terroristas u otras organizaciones, o personas subversivas cuyos fines puedan amenazar la seguridad de la Unión o de los Estados miembros).

▼B

8. Cuando proceda y de conformidad con las disposiciones legales y reglamentarias nacionales, se podrá considerar pertinente para la investigación de seguridad las circunstancias económicas o el historial médico de una persona.

9. Cuando proceda, y de conformidad con las disposiciones legales y reglamentarias nacionales, podrán también considerarse pertinentes para la investigación de seguridad la conducta y las circunstancias de un cónyuge, un cohabitante o un miembro de la familia cercana.

Requisitos de investigación a efectos del acceso a ICUE

Primera concesión de una habilitación de seguridad

10. La habilitación de seguridad inicial para acceder a información de los grados CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se basará en una investigación de seguridad que abarque un período de al menos los cinco últimos años, o bien desde que la persona cumplió los 18 años de edad hasta el tiempo presente, eligiendo el período más corto, y que incluya los siguientes aspectos:

a) cumplimentación de un cuestionario personal de seguridad nacional para el grado de ICUE a la que solicita tener acceso la persona investigada; una vez cumplimentado, el cuestionario se remitirá a la autoridad de seguridad competente;

b) comprobación de la identidad, ciudadanía o nacionalidad de la persona: se verificará la fecha y lugar de nacimiento de la persona y se comprobará su identidad. Se determinará la ciudadanía o nacionalidad, pasada y presente, de la persona; esta comprobación incluirá una evaluación de la posible vulnerabilidad frente a presiones de fuentes extranjeras, por ejemplo debido a su lugar de residencia anterior o a vinculaciones del pasado, y

c) comprobación de los registros nacionales y locales: se comprobarán los registros nacionales de seguridad y, si existe, el de antecedentes penales, u otros registros similares de las administraciones públicas y de la policía. Deberán comprobarse los registros policiales o judiciales con competencia territorial en los lugares donde haya residido o trabajado la persona investigada.

11. La habilitación de seguridad inicial para acceder a información clasificada de grado TRÈS SECRET UE/EU TOP SECRET se basará en una investigación de seguridad que abarque un período de al menos los diez últimos años, o bien desde que el solicitante cumplió 18 años de edad hasta el tiempo presente, eligiendo el período más corto. En caso de realizarse entrevistas conforme a lo previsto en la letra e), las investigaciones abarcarán un período de al menos los siete últimos años, o bien desde que la persona cumplió 18 años de edad hasta el tiempo presente, eligiendo el período más corto. Además de los criterios indicados en el punto 7, antes de conceder una HPS de grado TRÈS SECRET UE/EU TOP SECRET deberán realizarse indagaciones, en la medida en que lo permitan las disposiciones legales y reglamentarias nacionales, sobre los factores que se indican a continuación; estos factores también pueden ser pertinentes antes de conceder una HPS de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, cuando así lo exijan las disposiciones legales y reglamentarias nacionales:

a) situación económica: se investigará la situación económica de la persona, con el fin de evaluar si es vulnerable frente a posibles presiones de procedencia extranjera o nacional por sufrir dificultades económicas graves, o con el fin de descubrir ingresos económicos inexplicables;

▼B

b) educación: se investigará a fin de verificar los antecedentes académicos de la persona en escuelas, universidades y otros centros de enseñanza a los que haya asistido desde que haya cumplido 18 años de edad o durante el período que estime conveniente la autoridad que efectúa la investigación;

c) empleos: se investigará el trabajo actual y los anteriores, consultando registros e informes sobre rendimiento o eficiencia, y la opinión de los empleadores o superiores jerárquicos;

d) servicio militar: cuando proceda, se verificará la prestación del servicio militar de la persona y las circunstancias de su baja, y

e) entrevistas: siempre y cuando lo permita y prevea la legislación nacional, se mantendrán una o varias entrevistas con la persona. También se entrevistará a otras personas que estén en condiciones de hacer una valoración imparcial de los antecedentes, las actividades, la lealtad, honradez y fiabilidad del interesado. Si el procedimiento nacional implica la solicitud de garantes al sujeto de la investigación, se entrevistará a las personas que hayan aportado referencias, salvo que existan motivos justificados para no hacerlo.

12. Cuando sea necesario y de conformidad con las disposiciones legales y reglamentarias nacionales, podrán realizarse investigaciones adicionales con el fin de profundizar en toda la información pertinente de que se disponga sobre una persona y para confirmar o desmentir la información desfavorable.

Renovación de una habilitación de seguridad

13. Tras la concesión inicial de una habilitación de seguridad, y siempre que la persona haya prestado servicio de forma ininterrumpida en una administración nacional o en la SGC y siga necesitando acceder a ICUE, la habilitación de seguridad se revisará con vistas a su renovación por períodos no superiores a cinco años para las habilitaciones TRÈS SECRET UE/EU TOP SECRET, y a diez años para las habilitaciones SECRET UE/EU SECRET y CONFIDENTIEL UE/EU CONFIDENTIAL, contados a partir de la fecha de notificación del resultado de la última investigación de seguridad que haya servido de base para dichas habilitaciones. Todas las investigaciones de seguridad a efectos de la renovación de una habilitación de seguridad abarcarán el período transcurrido desde la anterior investigación de seguridad.

14. Para la renovación de las habilitaciones de seguridad se investigarán los factores señalados en los puntos 10 y 11.

15. Las solicitudes de renovación se cursarán con la debida antelación, teniendo en cuenta el tiempo necesario para efectuar las investigaciones de seguridad. No obstante, si la ANS pertinente u otra autoridad nacional competente hubiese recibido la oportuna solicitud de renovación y el correspondiente cuestionario personal de seguridad antes de que caduque la habilitación de seguridad y no hubiese finalizado la investigación de seguridad requerida, la autoridad nacional competente podrá, si así lo permiten las disposiciones legales y reglamentarias nacionales, prorrogar la validez de la habilitación de seguridad vigente por un plazo no superior a 12 meses. Si al término de este período de 12 meses la investigación de seguridad no hubiese concluido aún, la persona solo podrá desempeñar funciones que no requieran una habilitación de seguridad.

Procedimientos de autorización en la SGC

16. En el caso de los funcionarios y otros agentes de la SGC, la autoridad de seguridad de la SGC remitirá el cuestionario personal de seguridad, una vez cumplimentado, a la ANS del Estado miembro del que sea nacional la persona, requiriendo que se realice la investigación de seguridad correspondiente al grado de la ICUE para la que dicha persona requiera el acceso.

▼B

17. Cuando llegue a conocimiento de la SGC información pertinente para la investigación de seguridad sobre una persona que ha solicitado una habilitación de seguridad para acceder a ICUE, la SGC, actuando de acuerdo con las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS pertinente.

18. Una vez concluida la investigación de seguridad, la ANS pertinente comunicará el resultado de la investigación a la autoridad de seguridad de la SGC, empleando para ello el modelo normalizado de comunicación prescrito por el Comité de Seguridad.

    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 facultada para proceder a los nombramientos de la SGC podrá otorgarle una autorización para acceder a ICUE del grado pertinente hasta una fecha determinada.

    b) Si los resultados de la investigación de seguridad no aseguran dicha garantía, la autoridad facultada para proceder a los nombramientos de la SGC lo notificará a la persona, que podrá requerir ser oído por esta. La autoridad facultada para proceder a los nombramientos podrá pedir a la ANS competente cuantas aclaraciones le puedan facilitar, de conformidad con sus disposiciones legales y reglamentarias. De confirmarse el resultado anterior, no se concederá la autorización para acceder a ICUE.

19. La investigación de seguridad, junto con los resultados obtenidos deberá ser conforme a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión, incluido todo lo relativo a recursos. Se podrá apelar contra las decisiones de la autoridad facultada para proceder a los nombramientos de la SGC de acuerdo con lo dispuesto en el Estatuto de los funcionarios de la Unión Europea y el régimen aplicable a los otros agentes de la Unión Europea, establecido en el Reglamento (CEE, Euratom, CECA) nº 259/68 del Consejo ([1]) («el Estatuto de los funcionarios y régimen aplicable»).

20. Los expertos nacionales destinados en la SGC en comisión de servicio para un puesto que requiera acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior deberán presentar a la autoridad de seguridad de la SGC, antes de asumir sus funciones, un Certificado de Habilitación Personal de Seguridad (CHPS) válido para el acceso a ICUE, basándose en la cual la autoridad facultada para proceder a los nombramientos expedirá una autorización para acceder a ICUE.

21. La SGC aceptará la autorización de acceso a ICUE concedida por otra institución, órgano o agencia de la Unión, siempre que siga siendo válida. La autorización valdrá para cualquier nombramiento de la persona en la SGC. La institución, órgano o agencia de la Unión que esté contratando a la persona en cuestión notificará la ANS correspondiente del cambio de empleador.

22. 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 la SGC facultada para proceder a los nombramientos, 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 empleado en la SGC ni en la administración pública de un Estado miembro, el resultado de la investigación se remitirá de nuevo a la ANS correspondiente para que confirme que sigue siendo válido y adecuado.

23. Si la SGC tuviera conocimiento de que una persona que tiene autorización para acceder a ICUE representa un riesgo para la seguridad, la SGC, 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 de acceso a ICUE.

([1]) Reglamento (CEE, Euratom, CECA) nº 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (DO L 56 de 4.3.1968, p. 1).

▼B

24. Si una ANS notifica a la SGC la retirada de una garantía concedida de conformidad con el punto 18, letra a), a una persona que tiene autorización de acceso a ICUE, la autoridad facultada para proceder a los nombramientos de la SGC 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 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.

25. La decisión de retirar o suspender una autorización de acceso a ICUE a un funcionario u otro agente de la SGC y, en su caso, los motivos para hacerlo se comunicarán a la persona, que podrá requerir ser oído por la autoridad facultada para proceder a los nombramientos. 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 podrá apelar contra las decisiones de la autoridad facultada para proceder a los nombramientos de la SGC de acuerdo con lo dispuesto en el Estatuto de los funcionarios y régimen aplicable.

Registros de las habilitaciones de seguridad y las autorizaciones

26. Los Estados miembros y la SGC llevarán, respectivamente, registros de las HPS y de las autorizaciones que hayan concedido para acceder a información de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. Estos registros indicarán, como mínimo, el nivel de la ICUE al que el interesado puede tener acceso, la fecha de concesión de la habilitación de seguridad y su período de validez.

27. La autoridad de seguridad competente podrá expedir un CHPS que acredite a qué grado de ICUE puede tener acceso la persona (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), la fecha de validez de la HPS para acceder a ICUE o de la autorización para acceder a ICUE de que se trate y la fecha de caducidad del propio certificado.

Excepciones al requisito de titularidad de una HPS

28. El acceso a la ICUE de aquellas personas que en los Estados miembros estén debidamente autorizadas en virtud de sus funciones se determinará de conformidad con las disposiciones legales y reglamentarias nacionales; estas personas serán informadas de sus obligaciones respecto de la protección de la ICUE.

IV. FORMACIÓN Y SENSIBILIZACIÓN EN MATERIA DE SEGURIDAD

29. Todas las personas a las que se haya otorgado una habilitación de seguridad declararán por escrito que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias derivadas de un posible comprometimiento de esta información. Los Estados miembros y la SGC, según corresponda, llevarán un registro de estas declaraciones escritas.

30. Desde un principio, se sensibilizará 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 aleccionará periódicamente. Dichas personas deberán dar cuenta inmediatamente a las autoridades de seguridad correspondientes de cualquier actitud o actividad que consideren sospechosa o inusual.

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

V. CIRCUNSTANCIAS EXCEPCIONALES

32. Si así lo permiten las disposiciones legales y reglamentarias nacionales, una habilitación de seguridad otorgada por una autoridad de seguridad competente de un Estado miembro para el acceso a información clasificada nacional podrá permitir a funcionarios nacionales, de forma temporal y en espera

▼B

de la concesión de una HPS para acceder a ICUE, el acceso a ICUE de grado equivalente al especificado en el cuadro de equivalencias del apéndice B, siempre que dicho acceso temporal sea necesario para los intereses de la Unión. Cuando las disposiciones legales y reglamentarias nacionales no permitan dicho acceso temporal a la ICUE, las ANS informarán de ello al Comité de Seguridad.

33. Por razones de urgencia, cuando esté debidamente justificado en interés del servicio y en espera de la conclusión de una investigación de seguridad completa, la autoridad facultada para proceder a los nombramientos de la SGC podrá conceder a funcionarios y otros agentes de la SGC 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 la misma. 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 SGC llevará un registro de estas declaraciones escritas.

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

a) el superior jerárquico de la persona 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 disponga de una HPS o de una autorización para acceder a ICUE;

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, y

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

35. 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.

36. En circunstancias muy excepcionales, como misiones en un medio hostil o durante períodos de incremento de la tensión internacional, cuando así lo requieran medidas de urgencia, y en particular cuando estén en peligro vidas humanas, los Estados miembros y el Secretario General o el Secretario General Adjunto 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 habilitación de seguridad exigida, siempre que dicha autorización sea imprescindible y no existan dudas razonables sobre la lealtad, honradez y fiabilidad de la persona de que se trate. Dicha autorización se registrará, junto con una descripción de la información para la cual se haya autorizado el acceso.

▼B

37. 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 Unión 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.

38. El Comité de Seguridad será informado de los casos en los que se recurra el procedimiento establecido en los puntos 36 y 37.

39. Cuando las disposiciones legales y reglamentarias nacionales de un Estado miembro establezcan normas más estrictas en lo relativo a autorizaciones temporales, nombramientos provisionales, acceso único o acceso de urgencia a información clasificada, los procedimientos previstos en la presente sección se aplicarán únicamente dentro de los límites previstos en las correspondientes disposiciones legales y reglamentarias nacionales.

40. El Comité de Seguridad recibirá un informe anual sobre el recurso a los procedimientos establecidos en la presente sección.

VI. ASISTENCIA A REUNIONES DEL CONSEJO

41. A reserva de lo dispuesto en el punto 28, las personas que deban participar en reuniones del Consejo o de sus órganos preparatorios en las que se examine información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior solo podrán hacerlo previa comprobación de la situación de su habilitación de seguridad. En el caso de los delegados, un CHPS u otra prueba de habilitación de seguridad deberá ser remitido a la Oficina de Seguridad de la SGC por las autoridades correspondientes, o, de manera excepcional, ser presentado por el delegado afectado. Cuando proceda, podrá utilizarse una lista recapitulativa de nombres en la que figuren las pruebas pertinentes de su habilitación de seguridad.

42. Cuando, por razones de seguridad, se retire una HPS que permita acceder a ICUE a una persona cuyas funciones requieran la asistencia a sesiones del Consejo o a reuniones de los órganos preparatorios del Consejo, la autoridad competente informará de ello a la SGC.

VII. ACCESO POTENCIAL A ICUE

43. 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, se les aleccionará sobre los procedimientos de seguridad para la protección de la ICUE y se les instruirá acerca de sus obligaciones en materia de protección de la información que se les confíe.

▼B

ANEXO II

SEGURIDAD FÍSICA

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 8. 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. Las medidas de seguridad física aplicables se determinarán sobre la base de una evaluación de las amenazas realizada por las autoridades competentes. La SGC y cada uno de los Estados miembros aplicarán 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, y

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

4. Al aplicar el concepto de defensa en profundidad, las autoridades de seguridad competentes determinarán la combinación apropiada de las siguientes medidas de seguridad física que deben 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;

▼B

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. Podrá autorizarse a la autoridad competente para 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 del mismo. 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 competente se asegurará de que el equipo que se adquiera para la protección física de la ICUE (armarios de seguridad, trituradoras de papel, cerraduras, sistemas electrónicos de control de acceso, sistemas de detección de intrusos, sistemas de alarma) cumpla los estándares técnicos 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.

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:

▼B

a) zonas administrativas, y

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

En la presente Decisión, toda referencia a las zonas administrativas y a las zonas de acceso restringido, incluidas las zonas de acceso restringido protegidas por medios técnicos, se entenderá que incluye asimismo las equivalentes nacionales.

13. La autoridad de seguridad competente 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 sin escolta a las personas debidamente autorizadas por la autoridad competente, 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 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, estarán acompañados en todo momento y debidamente habilitados, salvo que se tomen medidas para que no sea posible que accedan a la ICUE.

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;

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

▼B

c) estas zonas serán objeto de inspecciones físicas o técnicas regularmente, según lo requiera la autoridad de seguridad competente; 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 punto 17, letra d), todos los equipos de comunicaciones y todos los aparatos eléctricos o electrónicos deberán ser examinados por la autoridad de seguridad competente antes de que puedan ser utilizados en zonas donde se estén celebrando reuniones o realizando trabajos en que se maneje información clasificada de grado SECRET UE/EU SECRET y superior, y cuando la amenaza para la ICUE se considere elevada, con el fin de garantizar que ninguna información en claro 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 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 competente 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

▼B

c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la ICUE de conformidad con los puntos 28 a 41 del anexo III y se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente para garantizar que la ICUE está protegida del 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 competente.

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 28 a 41 del anexo III,

ii) se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente para garantizar que el acceso a la ICUE se impide 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, bien dentro de un contenedor de seguridad o bien en una cámara acorazada.

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

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

a) en un contenedor de seguridad conforme a lo dispuesto en el punto 8, con al menos uno 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;

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

▼B

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

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

30. La autoridad de seguridad competente definirá procedimientos de gestión de las llaves y las combinaciones de las oficinas, salas, cámaras acorazadas y contenedores de seguridad. 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 hayan realizado operaciones de mantenimiento o reparación de una cerradura, y

e) al menos cada 12 meses.

▼B

ANEXO III

TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 9. Establece las medidas administrativas para controlar la ICUE a lo largo de su ciclo de vida con el fin de prevenir y detectar 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 será responsable de determinar el grado de clasificación de seguridad atendiendo a las directrices de clasificación pertinentes y de la difusión inicial de la información.

4. El grado de clasificación de la ICUE se determinará de conformidad con el artículo 2, apartado 2, y con referencia a la política de seguridad que se aprobará de conformidad con el artículo 3, apartado 3.

5. La clasificación de seguridad se indicará clara y correctamente, independientemente de que la ICUE sea verbal o figure en soporte de papel, electrónico o cualquier otro.

6. 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.

7. 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.

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. La clasificación de una carta o nota de transmisión de documentos será equivalente al mayor grado 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

10. Junto con una de las marcas de la clasificación de seguridad fijadas en el artículo 2, apartado 2, 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;

    c) marcas sobre posibilidad de cesión, o

▼B

d) en su caso, la fecha o acontecimiento específico tras los cuales podrá rebajarse el grado de clasificación o desclasificarse.

Marcas abreviadas de clasificación

11. 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.

12. 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
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Producción de ICUE

13. 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, y

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

14. Cuando no sea posible aplicar el punto 13 a una ICUE, se tomarán otras medidas adecuadas de conformidad con las directrices de seguridad que se establezcan con arreglo al artículo 6, apartado 2.

Reducción del grado de clasificación y desclasificación de la ICUE

15. 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.

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

III. REGISTRO DE LA ICUE A EFECTOS DE SEGURIDAD

17. Todo servicio administrativo de la SGC y de las administraciones públicas de los Estados miembros en que se maneje ICUE contará con un registro competente con el fin de garantizar que la ICUE se maneja 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 II.

▼B

18. A efectos de la presente Decisión, por registro a efectos de seguridad («registro») se entenderá la aplicación de procedimientos que registren el ciclo de vida del material de que se trate, incluida su difusión y destrucción.

19. Todo material clasificado de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior se inscribirá en registros especiales a su entrada o salida de un servicio administrativo.

20. El Registro Central de la SGC llevará un registro de toda la información clasificada cedida por el Consejo y la SGC a terceros Estados y organizaciones internacionales y de toda la información clasificada recibida de terceros Estados u organizaciones internacionales.

21. En el caso de un SIC, los procedimientos de registro podrán llevarse a cabo mediante procesos dentro del propio SIC.

22. El Consejo aprobará una política de seguridad sobre el registro de ICUE a efectos de seguridad.

Registros TRÈS SECRET UE/EU TOP SECRET

23. En los Estados miembros y en la SGC se establecerá un registro 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.

24. 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

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

26. 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.

27. Las medidas de seguridad aplicables a los documentos originales serán aplicables a sus copias y traducciones.

V. TRANSPORTE DE ICUE

28. El transporte de ICUE estará sujeto a las medidas de protección que se enuncian en los puntos 30 a 41. Cuando se transmita ICUE por medios electrónicos, y no obstante lo dispuesto en el artículo 9, apartado 4, las medidas de protección que figuran a continuación se completarán con las debidas contramedidas técnicas que prescriba la autoridad de seguridad competente, a fin de reducir al mínimo el riesgo de pérdida o compromiso.

29. Las autoridades de seguridad competentes de la SGC y de los Estados miembros emitirán instrucciones para el transporte de ICUE conforme a la presente Decisión.

Dentro de un edificio o grupo independiente de edificios

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

▼B

31. Dentro de un edificio o grupo independiente de edificios la información clasificada de grado TRÈS SECRET UE/EU TOP SECRET se transportará en sobre sellado en el que se indicará únicamente el nombre del destinatario.

Dentro de la Unión

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

33. El transporte de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET dentro de la Unión 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 estar en posesión del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el anexo II,

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

iii) se instruya al portador sobre sus responsabilidades en materia de seguridad, y

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 6, apartado 2.

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.

34. La información clasificada de grado RESTREINT UE/EU RESTRICTED podrá ser transportada también por servicios postales o servicios de mensajería comercial. Para el transporte de esta información no se precisa un certificado de correo.

35. 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 punto 33 deberá ser transportado como carga por empresas comerciales de transporte con arreglo a lo dispuesto en el anexo V.

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

Desde la Unión al territorio de un tercer Estado

37. La ICUE que se transporte desde la Unión al territorio de un tercer Estado irá empaquetada de forma que quede protegida de una revelación no autorizada.

▼B

38. El transporte de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y de grado SECRET UE/EU SECRET desde la Unión al territorio de un tercer Estado 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 estar en posesión del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el anexo II,

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

v) se instruya al portador sobre sus responsabilidades en materia de seguridad.

39. El transporte de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y de grado SECRET UE/UE SECRET cedida por la Unión 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 convenio conforme al artículo 13, apartado 2, letras a) o b).

40. La información clasificada de grado RESTREINT UE/EU RESTRICTED podrá ser transportada también por servicios postales o servicios de mensajería comercial.

41. El transporte de información clasificada de grado TRÈS SECRET UE/EU TOP SECRET desde la Unión hasta el territorio de un tercer Estado se efectuará por correo militar o diplomático.

VI. DESTRUCCIÓN DE ICUE

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

43. Los documentos sujetos a registro de conformidad con el artículo 9, apartado 2, 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.

44. 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.

45. 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.

46. Los documentos clasificados, incluidos los de grado RESTREINT UE/EU RESTRICTED, se destruirán por métodos que cumplan las normas de la Unión pertinentes o normas equivalentes o que hayan sido homologados por

▼B

los Estados miembros de conformidad con las normas técnicas nacionales, a fin de impedir su reconstrucción total o parcial.

47. La destrucción de los soportes de almacenamiento informático utilizados para la ICUE se realizará de conformidad con el punto 37 del anexo IV.

48. En caso de emergencia, y de haber un riesgo inminente de revelación no autorizada, la ICUE será destruida por el poseedor, de tal modo que no pueda reconstruirse ni total ni parcialmente. Se informará al originador y al registro originador de la destrucción de emergencia de la ICUE registrada.

VII. VISITAS DE EVALUACIÓN

49. El término «visita de evaluación» se empleará en lo sucesivo para designar:

a) toda inspección o visita de evaluación realizada de conformidad con el artículo 9, apartado 3, y el artículo 16, apartado 2, letras e), f) y g), o

b) toda visita de evaluación realizada de conformidad con el artículo 13, apartado 5,

a fin de verificar la eficacia de las medidas establecidas para la protección de la ICUE.

50. Las visitas de evaluación se realizarán, entre otros fines, para:

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

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

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

d) reforzar los programas de formación y de sensibilización en materia de seguridad que ya realicen las autoridades de seguridad.

51. Antes del término de cada año natural, el Consejo adoptará el programa de visitas de evaluación para el año siguiente prescrito en el artículo 16, apartado 1, letra c). Las fechas concretas de cada visita de evaluación se determinarán de común acuerdo con el órgano o la agencia de la Unión, el Estado miembro, el tercer Estado o la organización internacional afectados.

Realización de las visitas de evaluación

52. Las visitas de evaluación se llevarán a cabo con el fin de comprobar el cumplimiento de las normas, reglamentaciones y procedimientos pertinentes de la entidad visitada y verificar si las prácticas de dicha entidad se ajustan a los principios básicos y las normas mínimas establecidas en la presente Decisión y a las disposiciones que rigen el intercambio de información clasificada con dicha entidad.

53. Las visitas de evaluación se efectuarán en dos fases. Antes de la visita propiamente dicha se celebrará una reunión preparatoria con la entidad afectada, si procede. Tras esta reunión preparatoria, el equipo de evaluación establecerá, de común acuerdo con la entidad afectada, un programa detallado para la visita de evaluación que abarque todos los aspectos de la seguridad. El equipo de evaluación debe tener acceso a todos los locales, en particular a los registros y puntos de presencia de los SIC, en los que se maneje ICUE.

54. Las visitas de evaluación a las administraciones públicas de los Estados miembros, terceros Estados y organizaciones internacionales se efectuarán en plena colaboración con los funcionarios de la entidad, del tercer Estado o de la organización internacional visitados.

▼B

55. Las visitas de evaluación a los órganos, agencias y entidades de la Unión que apliquen la presente Decisión o sus principios se efectuarán con asistencia de expertos de la ANS del país en que esté establecido el órgano o la agencia.

56. En el caso de las visitas de evaluación a órganos, agencias y entidades de la Unión que apliquen la presente Decisión o sus principios, y a terceros Estados y organizaciones internacionales, se podrá solicitar la asistencia y contribución de expertos de la ANS, de conformidad con las medidas de aplicación que debe acordar el Comité de Seguridad.

Informes

57. Al término de la visita de evaluación se presentarán a la entidad visitada las principales conclusiones y recomendaciones. A continuación, se elaborará un informe de la visita de evaluación. Cuando se hayan propuesto medidas correctoras y recomendaciones, el informe incluirá datos suficientes que avalen sus conclusiones. El informe se remitirá a la autoridad que corresponda de la entidad visitada.

58. Con respecto a las visitas de evaluación realizadas en las administraciones públicas de los Estados miembros:

a) el proyecto de informe de evaluación se remitirá a las ANS de que se trate para que verifiquen que no contiene errores en cuanto a los hechos ni información clasificada de grado superior a RESTREINT UE/EU RESTRICTED, y

b) salvo cuando la ANS del Estado miembro afectado solicite que no se efectúe una difusión general, los informes de evaluación se distribuirán al Comité de Seguridad. El informe llevará el grado de clasificación RESTREINT UE/EU RESTRICTED.

Se elaborará un informe periódico, bajo la responsabilidad de la Oficina de Seguridad de la SGC, para destacar las principales enseñanzas extraídas de las visitas de evaluación realizadas en los Estados miembros a lo largo de un período determinado; el informe será examinado por el Comité de Seguridad.

59. Cuando se trate de visitas de evaluación a terceros Estados u organizaciones internacionales, el informe se remitirá al Comité de Seguridad. Esos informes llevarán la clasificación, como mínimo, de grado RESTREINT UE/EU RESTRICTED. En las visitas de seguimiento se comprobará la aplicación de las medidas correctoras y se informará de ella al Comité de Seguridad.

60. Cuando se trate de visitas de evaluación a todo órgano, agencia y entidad de la Unión que aplique la presente Decisión o sus principios, los informes de las visitas de evaluación se distribuirán al Comité de Seguridad. Los proyectos de informes de las visitas de evaluación se remitirán a la agencia u órgano de que se trate para que verifique que no contienen errores en cuanto a los hechos ni información clasificada de grado superior a RESTREINT UE/EU RESTRICTED. En las visitas de seguimiento se comprobará la aplicación de las medidas correctoras y se informará de ella al Comité de Seguridad.

61. La Oficina de Seguridad de la SGC realizará inspecciones periódicas de los servicios administrativos de la SGC a los fines establecidos en el punto 50.

Lista de control

62. Corresponderá a la Oficina de Seguridad de la SGC elaborar y actualizar una lista de control de los puntos que deberán comprobarse en el curso de una visita de evaluación. Esta lista y sus eventuales actualizaciones se remitirán al Comité de Seguridad.

63. La información para completar la lista de control se obtendrá, en particular durante la visita, 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.

▼B

ANEXO IV

PROTECCIÓN DE LA ICUE MANEJADA EN LOS SIC

I. INTRODUCCIÓN

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

2. Las siguientes propiedades y conceptos relativos a la GI se consideran esenciales para la seguridad y correcto funcionamiento de las operaciones realizadas en los 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 o 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 GI

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 políticas y directrices de seguridad para la 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 examinarán las amenazas potenciales para el SIC y mantendrán evaluaciones de la amenaza actualizadas y exactas que reflejen el entorno operativo del momento. 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 (TI).

6. El tratamiento del riesgo de seguridad tendrá por objeto aplicar un conjunto de medidas de seguridad que creen un equilibrio satisfactorio entre las necesidades de los usuarios, el coste y el riesgo de seguridad residual.

7. Los requisitos específicos, escala y grado de detalle determinados por la autoridad de acreditación de seguridad 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.

▼B

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. Cualquier 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 y verificar que esos sistemas están correctamente aplicados, integrados y configurados.

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. La SGC y los Estados miembros colaborarán 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 SIC se basará en las enseñanzas obtenidas por las entidades que intervienen en la GI tanto dentro de la Unión como fuera de ella.

15. La difusión y ulterior aplicación de las mejores prácticas contribuirán a lograr un nivel equivalente de garantía en los distintos SIC que manejan ICUE y que funcionan en la SGC y en los Estados miembros.

Defensa en profundidad

16. Para paliar los riesgos en 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 que se ha producido un ataque a un SIC;

    d) *resistencia:* 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 de estas medidas de seguridad se determinará mediante una evaluación del riesgo.

17. La ANS u otra autoridad competente se asegurará:

    a) de que se pongan en práctica capacidades de ciberdefensa a fin de responder a amenazas que puedan traspasar los límites de las organizaciones o las fronteras nacionales, y

▼B

b) de que se coordinen las respuestas y de que se comparta la información sobre dichas amenazas, los 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 esenciales 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 efectúa un SIC, cuando es 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 disponibles constituye la primera línea de defensa de la seguridad de los SIC. En particular, todas las personas que intervienen en el ciclo de vida de un SIC, incluidos sus usuarios, deben ser conscientes:

a) de que los fallos de seguridad pueden perjudicar seriamente al SIC;

b) de los posibles daños a terceros que pueden derivarse de la interconectividad e interdependencia, y

c) de 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 son conscientes de las responsabilidades que conlleva la seguridad, será obligatoria la formación y concienciación en relación con la GI para todo el personal implicado, tanto los altos directivos como los usuarios de SIC.

Evaluación y aprobación de los productos de seguridad de TI

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 deben incluirse principalmente la evaluación, los controles y las auditorías.

25. Los productos criptológicos de protección de la ICUE serán evaluados y aprobados por una ACC de un Estado miembro.

26. Antes de recomendarlos para su aprobación por el Consejo o el Secretario General, de conformidad con el artículo 10, apartado 6, dichos productos criptológicos 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. El Consejo aprobará una política de seguridad sobre la evaluación y aprobación de los productos criptológicos.

27. Cuando ello esté justificado por motivos operativos específicos, el Consejo o el Secretario General, según proceda, podrá, previa recomendación del Comité de Seguridad, dispensar del cumplimiento de los requisitos recogidos en los puntos 25 o 26 del presente anexo y otorgar una aprobación provisional durante un período específico, de conformidad con el procedimiento establecido en el artículo 10, apartado 6.

▼B

28. El Consejo, por recomendación del Comité de Seguridad, podrá aceptar el proceso de evaluación, selección y aprobación de los productos criptológicos de un tercer Estado o de una organización internacional y considerar en consecuencia que tales productos criptológicos quedan aprobados a efectos de protección de ICUE cedida a dicho tercer Estado o dicha organización internacional.

29. Una ADA será una ACC de un Estado miembro, acreditada mediante criterios objetivos establecidos por el Consejo para realizar la segunda evaluación de los productos criptológicos de protección de la ICUE.

30. El Consejo aprobará una política de seguridad sobre la cualificación y aprobación de productos de seguridad de TI no criptológicos.

Transmisión dentro de zonas de acceso restringido y zonas administrativas

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

Interconexión segura de los SIC

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

33. Todo SIC tratará como no fiable a cualquier sistema de TI interconectado y aplicará medidas protectoras para controlar el intercambio de información clasificada.

34. Con relación a todas las interconexiones de un SIC con otro sistema de TI, se observarán los siguientes requisitos básicos:

a) las autoridades competentes enunciarán y aprobarán los requisitos operacionales 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.

35. 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 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 criptológico aprobado en conformidad con el artículo 10, se considerará que la conexión no es una interconexión.

36. 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

37. Los soportes de almacenamiento informático se destruirán con arreglo a un procedimiento aprobado por la autoridad de seguridad competente.

▼B

38. La reutilización, la reducción del grado de clasificación y la desclasificación de los soportes de almacenamiento informático se efectuarán de conformidad con unas directrices de seguridad establecidas de conformidad con el artículo 6, apartado 2.

Circunstancias de emergencia

39. No obstante lo dispuesto en la presente Decisión, podrán aplicarse 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.

40. La ICUE podrá transmitirse utilizando productos criptológicos que hayan sido certificados para un grado de clasificación inferior o sin cifrar con el consentimiento de la autoridad competente, si resulta evidente que un retraso podría causar un daño superior al que acarrea la revelación del material clasificado y si:

a) el emisor y el receptor carecen de los medios de cifra requeridos o carecen de todo medio de cifra, y

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

41. 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.

42. Si hubiera que recurrir a lo expuesto en el punto 39, se presentará posteriormente un informe a la autoridad competente y al Comité de Seguridad.

III. GARANTÍA DE LA INFORMACIÓN: FUNCIONES Y AUTORIDADES

43. En los Estados miembros y en la SGC se establecerán las siguientes funciones respecto de la GI. 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

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

a) establecer políticas y 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 normas que rigen su idoneidad y selección;

d) garantizar que los productos criptológicos se seleccionen de conformidad con las normas 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 agentes en el ámbito de la seguridad y a los representantes de los usuarios sobre las políticas y directrices de seguridad relativas a la garantía de la información, y

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

▼B

Autoridad TEMPEST

45. 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 ICUE de un determinado grado de clasificación dentro de su entorno operativo.

Autoridad de Certificación Criptológica

46. Corresponderá a la Autoridad de Certificación Criptológica (ACC) garantizar que los productos criptológicos cumplan la política criptológica nacional o la del Consejo. Dará su aprobación a los productos criptológicos para tratar ICUE de un determinado grado de clasificación dentro de su entorno operativo. Por lo que se refiere a los Estados miembros, la ACC se encargará de evaluar los productos criptológicos.

Autoridad de Distribución Criptológica

47. 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 se hagan en condiciones de seguridad, y

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

Autoridad de Acreditación de Seguridad

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

a) velar por que los SIC cumplan las políticas y 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 políticas 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 políticas de seguridad del Consejo;

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 sensibles en relación con los SIC;

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

▼B

h) aprobar la interconexión de un SIC a otros 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 el riesgo residual, así como sobre las condiciones de la declaración de aprobación.

49. Corresponderá a la AAS de la SGC la acreditación de todos los SIC que funcionen en el marco del mandato de la SGC.

50. Corresponderá a la AAS competente de un Estado miembro acreditar los SIC y los componentes de estos que operen dentro de su jurisdicción.

51. Un Panel de Acreditación de Seguridad se encargará de la acreditación de los SIC que entren dentro de la competencia tanto de la AAS de la SGC 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 Comisión. Se invitará a asistir a otras entidades conectadas a un SIC, cuando dicho sistema se someta a debate.

El Panel de Acreditación de Seguridad estará presidido por un representante de la AAS de la SGC. 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 y le comunicará todas las declaraciones de acreditación.

Autoridad Operacional de Garantía de la Información

52. Corresponderá a la Autoridad Operacional de Garantía de la Información (AOGI) de cada sistema:

a) elaborar documentación de seguridad en consonancia con las políticas y 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 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 lo requiera la Autoridad de Acreditación de Seguridad (AAS);

g) proporcionar formación sobre la GI específica para SIC, y

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

▼B

ANEXO V

SEGURIDAD INDUSTRIAL

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 11, 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 duración de los contratos clasificados adjudicados por la Secretaría General del Consejo.

2. El Consejo 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 convocar una licitación o adjudicar un contrato clasificado, la SGC, 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, la SGC 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, la SGC 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 general de clasificación del contrato no podrá ser inferior al mayor grado 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, la SGC actuará de enlace con las ANS o las ASD de los Estados miembros o 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 seguridad, la cual, cuando proceda, incluirá la guía de clasificación de seguridad y será parte integrante de un contrato o subcontrato clasificado.

6. La cláusula sobre aspectos de la seguridad incluirá asimismo las disposiciones que exigirán del contratista o subcontratista el cumplimiento de los estándares mínimos que se establecen en la presente Decisión. El incumplimiento de dichos estándares mínimos podrá ser motivo suficiente para la rescisión del contrato.

Instrucciones de seguridad de un programa o proyecto

7. Según cuál sea el 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 emitir unas instrucciones de seguridad específicas del programa o proyecto. Estas instrucciones requerirán la aprobación de las ANS o de las ASD de los

▼B

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 habilitación de seguridad de establecimiento será concedida por la ANS o la ASD o cualquier otra autoridad de seguridad competente de un Estado miembro 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). Dicha habilitación se presentará a la SGC, como autoridad contratante, antes de facilitar o conceder acceso a la ICUE a un contratista o subcontratista, o a un posible contratista o subcontratista.

9. Al expedir una habilitación de seguridad de establecimiento, la ANS o la ASD competente procederá, como mínimo, a:

a) evaluar la integridad de la sociedad industrial u otro tipo de entidad;

b) evaluar la propiedad, el control o cualquier posible influencia indebida que pueda considerarse un riesgo para la seguridad;

c) verificar que la sociedad industrial u otro tipo de entidad ha implantado un sistema de seguridad en el establecimiento que aplica todas las medidas de seguridad apropiadas necesarias para la protección de la información o el material clasificados de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, de conformidad con los requisitos prescritos en la presente Decisión;

d) verificar que la situación de seguridad de los directivos, los propietarios y los empleados que necesitan acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se ha establecido de conformidad con los requisitos prescritos en la presente Decisión, y

e) verificar que la sociedad industrial u otro tipo de entidad ha nombrado un agente de seguridad del establecimiento, que responda ante su dirección de la observancia de las obligaciones en cuanto a la seguridad.

10. Cuando proceda, la SGC, 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.

11. La autoridad contratante no adjudicará un contrato clasificado al licitador seleccionado antes de 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.

12. La ANS o la ASD o cualquier otra autoridad de seguridad competente que haya expedido una habilitación de seguridad de establecimiento notificará a la SGC, como autoridad contratante, los cambios que afecten a dicha

▼B

habilitación. En el caso de los subcontratos, se informará al respecto a la ANS, la ASD o cualquier otra autoridad de seguridad competente.

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

IV. CONTRATOS Y SUBCONTRATOS CLASIFICADOS

14. Cuando se facilite ICUE a un licitador en la fase precontractual, el pliego de condiciones 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.

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

16. En caso de rescisión de un contrato de este tipo, la SGC, como autoridad contratante (o la ANS, la ASD o cualquier otra autoridad de seguridad competente, según proceda, en el caso de una subcontratación), lo notificarán cuanto antes a los correspondientes organismos o autoridades competentes del Estado miembro en que esté registrado el contratista o subcontratista.

17. Por regla general, el contratista o subcontratista estará obligado a devolver a la autoridad contratante, al término del contrato o subcontrato clasificado, toda la ICUE que obre en su posesión.

18. La cláusula sobre aspectos de la seguridad establecerá disposiciones específicas para la eliminación de ICUE durante la ejecución del contrato o al término de este.

19. Cuando el contratista o subcontratista esté autorizado a conservar ICUE tras la terminación 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.

20. Las condiciones en que un contratista podrá subcontratar se definirán en el pliego de condiciones y en el contrato.

21. Antes de subcontratar cualquier parte de un contrato clasificado, el contratista deberá obtener de la SGC, 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 Unión y no haya celebrado un acuerdo de seguridad de la información con esta.

22. El contratista responderá de que todas las actividades subcontratadas se ejecuten de conformidad con las normas mínimas prescritas en la presente Decisión y no transmitirá ICUE a ningún subcontratista sin el previo consentimiento escrito de la autoridad contratante.

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

▼B

V. VISITAS EN RELACIÓN CON CONTRATOS CLASIFICADOS

24. Cuando el personal de la SGC, de los contratistas o de los subcontratistas necesite 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 cualquier otra autoridad de seguridad competente. No obstante, en el contexto de proyectos específicos, las ANS o las ASD podrán también acordar un procedimiento que permita organizar directamente dichas visitas.

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

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

VI. TRANSMISIÓN Y TRANSPORTE DE ICUE

27. Por lo que se refiere a la transmisión de ICUE por medios electrónicos, se aplicarán las disposiciones pertinentes del artículo 10 y del anexo IV.

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

29. 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 mayor grado de clasificación del material que contenga;

c) se obtendrá una habilitación de seguridad de establecimiento del grado adecuado para las sociedades encargadas del transporte. En esos casos, el personal que se ocupe del envío deberá estar habilitado de conformidad con el anexo I;

d) antes de efectuarse 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 la ANS, la ASD o cualquier otra autoridad de seguridad competente afectada;

e) en la medida de lo posible, los viajes evitarán las paradas intermedias y se completarán con toda la rapidez que 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 de la ANS, la ASD o cualquier otra autoridad de seguridad competente tanto del Estado remitente como del destinatario.

VII. TRANSMISIÓN DE ICUE A CONTRATISTAS ESTABLECIDOS EN TERCEROS ESTADOS

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

▼B

VIII. INFORMACIÓN CLASIFICADA RESTREINT UE/EU RESTRICTED

31. La SGC, como autoridad contratante, en colaboración con la ANS o la ASD del Estado miembro, según proceda, estará facultada para realizar inspecciones 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.

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

33. Para los contratos adjudicados por la SGC 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.

34. La SGC, 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.

35. Las condiciones en que el contratista podrá subcontratar deberán estar en conformidad con el punto 21.

36. Cuando un contrato suponga el manejo de información clasificada de grado RESTREINT UE/EU RESTRICTED en un SIC gestionado por un contratista, la SGC, 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 sean 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.

▼B

ANEXO VI

INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 13.

II. MARCOS QUE REGULAN EL INTERCAMBIO DE INFORMACIÓN CLASIFICADA

2. Cuando el Consejo haya determinado que existe la necesidad de intercambiar información clasificada de forma prolongada,

— se celebrará un acuerdo de seguridad de la información, o

— se celebrará un acuerdo administrativo,

de conformidad con el artículo 13, apartado 2, y las secciones III y IV y sobre la base de una recomendación del Comité de Seguridad.

3. Cuando la ICUE generada a efectos de una operación PCSD deba comunicarse a terceros Estados u organizaciones internacionales que participen en dicha operación, y cuando no exista ninguno de los marcos a que se refiere el punto 2, el intercambio de ICUE con el tercer Estado u organización internacional de que se trate se regulará, conforme a lo dispuesto en la sección V, por:

— un acuerdo marco de participación,

— un acuerdo de participación *ad hoc*, o

— de no existir alguno de estos, un acuerdo administrativo *ad hoc.*

4. En ausencia de uno de los marcos a que se refieren los puntos 2 y 3, y cuando se adopte la decisión de ceder ICUE a un tercer Estado u organización internacional con arreglo a un procedimiento *ad hoc* de carácter excepcional de conformidad con lo dispuesto en la sección VI, se pedirán garantías por escrito al tercer Estado u organización internacional interesado de que mantendrá protegida la ICUE que se le ceda de acuerdo con los principios básicos y las normas mínimas establecidas por la presente Decisión.

III. ACUERDOS DE SEGURIDAD DE LA INFORMACIÓN

5. Los acuerdos de seguridad de la información establecerán los principios básicos y las normas mínimas aplicables al intercambio de información clasificada entre la Unión y un tercer Estado u organización internacional.

6. Los acuerdos de seguridad de la información establecerán las disposiciones técnicas de aplicación que deban convenirse entre las autoridades de seguridad competentes de las instituciones y órganos pertinentes de la Unión y la autoridad de seguridad competente del tercer Estado u organización internacional de que se trate. Dichas disposiciones tendrán debidamente en cuenta el grado de protección que ofrezcan las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional de que se trate. Serán aprobadas por el Comité de Seguridad.

7. Con arreglo a un acuerdo de seguridad de la información, no se intercambiará ICUE por medios electrónicos a menos que se haya previsto explícitamente en el acuerdo o en las disposiciones técnicas de aplicación correspondientes.

8. En los acuerdos sobre seguridad de la información que celebre el Consejo se designará un registro en cada parte como punto principal de entrada y salida para los intercambios de información clasificada.

▼B

9. Con el fin de evaluar la eficacia de las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional en cuestión, se efectuarán visitas de evaluación de común acuerdo con el tercer Estado o la organización internacional de que se trate. Dichas visitas se realizarán de conformidad con las disposiciones pertinentes del anexo III y evaluarán:

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

   b) las características propias de la política de seguridad y la manera en que se organiza la seguridad en el tercer Estado u organización internacional, que pueden influir en el grado de la información clasificada que pueda intercambiarse;

   c) las medidas y procedimientos de seguridad que se aplican efectivamente, y

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

10. El equipo que efectúe la visita de evaluación en nombre de la Unión evaluará si las normas y procedimientos de seguridad en el tercer Estado o la organización internacional son adecuados para ofrecer protección a la ICUE de un determinado nivel.

11. Los resultados de estas visitas se recogerán en un informe que servirá de base al Comité de Seguridad para determinar el grado máximo de la ICUE que podrá intercambiarse en papel o, cuando proceda, de forma electrónica, con el tercero de que se trate, así como las condiciones específicas de dicho intercambio.

12. Deberá ponerse el máximo empeño en realizar una visita completa de evaluación de la seguridad en el tercer Estado u organización internacional de que se trate antes de que el Comité de Seguridad apruebe las disposiciones de aplicación, con objeto de determinar la naturaleza y la eficacia del sistema de seguridad que esté establecido. No obstante, cuando ello no resulte posible, el Comité de Seguridad recibirá un informe lo más completo posible de la Oficina de Seguridad de la SGC, basado en la información de que disponga, en el que se le informará de la normativa de seguridad aplicable y de la manera en que está organizada la seguridad en el tercer Estado o la organización internacional de que se trate.

13. El informe de la visita de evaluación o, en caso de no existir dicho informe, el informe a que se refiere el punto 12, se remitirá al Comité de Seguridad, que deberá considerarlo satisfactorio, antes de que se ceda efectivamente ICUE al tercer Estado o a la organización internacional de que se trate.

14. Las autoridades de seguridad competentes de las instituciones y órganos de la Unión comunicarán al tercer Estado u organización internacional la fecha a partir de la cual la Unión se encontrará en condiciones de ceder información clasificada de la Unión con arreglo al acuerdo, así como el máximo grado de ICUE que pueda intercambiarse en soporte de papel o por medios electrónicos.

15. Si se juzga necesario, se efectuarán visitas de seguimiento, en particular si:

   a) es necesario elevar el grado en que se cede la ICUE, o

   b) se han notificado a la Unión cambios fundamentales en las medidas de seguridad del tercer Estado u organización internacional que puedan afectar al modo en que protege la ICUE, o

   c) se ha producido un incidente grave que implique revelación no autorizada de ICUE.

▼B

16. Una vez que el acuerdo de seguridad de la información esté en vigor y se haya intercambiado información clasificada con el tercer Estado o la organización internacional de que se trate, el Comité de Seguridad podrá decidir modificar el grado máximo de la ICUE que podrá ser intercambiada en papel o por medios electrónicos, en particular, como consecuencia de posibles visitas de evaluación ulteriores.

IV. ACUERDOS ADMINISTRATIVOS

17. Cuando exista la necesidad de intercambiar durante largo tiempo información clasificada, en principio, de un grado no superior a RESTREINT UE/EU RESTRICTED con un tercer Estado o una organización internacional y el Comité de Seguridad 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 Secretario General podrá, previa aprobación del Consejo, celebrar un acuerdo administrativo, en nombre de la SGC, con las autoridades competentes del tercer Estado o la organización internacional.

18. Cuando por motivos operativos urgentes sea necesario establecer rápidamente un marco de intercambio de información clasificada, el Consejo podrá decidir, con carácter excepcional, que se celebre un acuerdo administrativo para el intercambio de información de un grado de clasificación superior.

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

20. Antes de ceder efectivamente ICUE al tercer Estado o la organización internacional de que se trate, se realizará una visita de evaluación con arreglo al punto 9 y se remitirá el correspondiente informe o, en caso de no existir dicho informe, el informe a que se refiere el punto 12, al Comité de Seguridad, que deberá considerarlo satisfactorio.

21. Con arreglo a un acuerdo administrativo, no se intercambiará ICUE por medios electrónicos a menos que se haya establecido explícitamente en el acuerdo.

V. INTERCAMBIO DE INFORMACIÓN CLASIFICADA EN EL CONTEXTO DE LAS OPERACIONES PCSD

22. La participación de terceros Estados o de organizaciones internacionales en operaciones PCSD se rige por acuerdos marco de participación. Los citados acuerdos incluirán disposiciones en materia de cesión de ICUE generada con motivo de operaciones PCSD a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

23. Los acuerdos de participación *ad hoc* celebrados para una operación PCSD específica incluirán disposiciones sobre la cesión de ICUE generada a efectos de dicha operación a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

▼B

24. A falta de acuerdo de seguridad de la información, y a la espera de la celebración de un acuerdo de participación, la cesión de ICUE, generada a efectos de la operación, a un tercer Estado u organización internacional participante en la operación, se regulará mediante un acuerdo administrativo que celebrará el Alto Representante o será objeto de una decisión sobre cesión *ad hoc* de conformidad con la sección VI. Con arreglo a dicho acuerdo solo se intercambiará ICUE mientras se siga contemplando la participación del tercer Estado o de la organización internacional. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

25. Las disposiciones sobre la información clasificada que deberán figurar en los acuerdos marco de participación, en los acuerdos de participación *ad hoc* y en los acuerdos administrativos *ad hoc* a que se refieren los puntos 22, 23 y 24 establecerán que el tercer Estado u organización internacional afectado deberá garantizar que su personal destinado en comisión de servicio a la operación protegerá la ICUE con arreglo a las normas de seguridad del Consejo y con cualquier otra directriz emitida por las autoridades competentes, incluida la cadena de mando de la operación.

26. 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 las disposiciones en materia de intercambio de información clasificada establecidas 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.

27. No se permitirá el intercambio de ICUE por medios electrónicos con arreglo a un acuerdo marco de participación, un acuerdo de participación *ad hoc* o un acuerdo administrativo *ad hoc* con un tercer Estado u organización internacional, a menos que se haya establecido explícitamente en el acuerdo o en el acuerdo administrativo en cuestión.

28. 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 22 a 27. 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.

29. A falta de un acuerdo de seguridad de la información, y en caso de necesidad operativa específica e inmediata, la cesión de ICUE al Estado anfitrión en cuyo territorio se lleve a cabo una operación PCSD podrá regularse mediante un acuerdo administrativo que celebrará el Alto Representante. Esta posibilidad se dispondrá en la decisión que establezca la operación PCSD. La ICUE cedida en esas circunstancias se limitará a la generada para los fines de la operación PCSD y su grado de clasificación no será superior a RESTREINT UE/EU RESTRICTED, salvo que se disponga un grado de clasificación superior en la decisión que establezca la operación PCSD. En el marco del citado acuerdo administrativo, se exigirá al Estado de acogida que se comprometa a proteger la ICUE respetando normas mínimas no menos estrictas que las establecidas por la presente Decisión.

▼B

30. A falta de acuerdo de seguridad de la información, la cesión de ICUE a un tercer Estado y a organizaciones internacionales pertinentes, distintos de los participantes en una operación PCSD, podrá regularse mediante un acuerdo administrativo que celebrará la Alta Representante. Si resulta conveniente, se preverá dicha posibilidad y toda condición al respecto en la decisión que establezca la operación PCSD. La ICUE cedida en esas circunstancias se limitará a la generada para los fines de la operación PCSD y su grado de clasificación no será superior a RESTREINT UE/EU RESTRICTED, salvo que se establezca un grado de clasificación superior en la decisión que establezca la operación PCSD. En el marco del citado acuerdo administrativo, se pedirá al tercer Estado o a la organización internacional de que se trate que se comprometan a proteger la ICUE respetando normas mínimas no menos estrictas que las establecidas por la presente Decisión.

31. No será preciso establecer disposiciones de aplicación ni efectuar visitas de evaluación antes de aplicar las disposiciones en materia de cesión de ICUE en el contexto de los puntos 22, 23 y 24.

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

32. En caso de que no exista un marco de conformidad con las secciones III, IV y V, y cuando el Consejo o uno de sus órganos preparatorios determine que es necesario, a título excepcional, ceder ICUE a un tercer Estado o a una organización internacional, la SGC:

a) comprobará, en la medida de lo posible, en colaboración con las autoridades de seguridad del tercer Estado u organización internacional de que se trate, que su normativa, estructuras y procedimientos de seguridad garantizan que la ICUE que se les ceda será protegida con arreglo a estándares no menos estrictos que los establecidos por la presente Decisión, e

b) invitará al Comité de Seguridad a emitir, basándose en la información disponible, una recomendación sobre el grado de confianza que deba concederse a la normativa, estructuras y procedimientos de seguridad del tercer Estado u organización internacional a la que se comunique ICUE.

33. Si el Comité de Seguridad emite una recomendación a favor de la cesión de la ICUE, el asunto se comunicará al Comité de Representantes Permanentes (Coreper), que deberá tomar una decisión sobre la cesión de dicha información.

34. Si la recomendación del Comité de Seguridad no es favorable a la cesión de la ICUE:

a) para los asuntos relacionados con la PESC o la PCSD, el Comité Político y de Seguridad examinará el asunto y formulará una recomendación al Coreper para que este tome una decisión;

b) para todos los demás asuntos, el Coreper examinará el asunto y tomará una decisión.

35. Cuando se considere apropiado, y siempre que se cuente con el consentimiento previo por escrito del originador, el Coreper podrá decidir que la información clasificada sea cedida solo en parte o únicamente si se ha reducido el grado de clasificación o se ha desclasificado previamente; o que la información que deba cederse se elabore sin hacer referencia a la fuente o al grado de clasificación UE original.

36. Una vez que se haya tomado la decisión de ceder ICUE, la SGC enviará el documento de que se trate, el cual deberá llevar una marca de posibilidad de cesión que indique a qué tercer Estado u organización internacional ha sido cedido. Antes o en el momento de la cesión efectiva, el tercero de que se trate se comprometerá por escrito a proteger la ICUE que reciba de acuerdo con los principios básicos y las normas mínimas que se establecen en la presente Decisión.

▼B

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

37. Cuando exista un marco para el intercambio de información clasificada con un tercer Estado u organización internacional con arreglo al punto 2, el Consejo tomará una decisión que autorice al Secretario General a ceder ICUE al tercer Estado o la organización internacional de que se trate, respetando el principio del consentimiento previo del originador. El Secretario General podrá delegar tal autorización en altos funcionarios de la SGC.

38. Cuando exista un acuerdo de seguridad de la información, con arreglo al punto 2, primer inciso, el Consejo podrá adoptar una decisión que autorice al Alto Representante a ceder al tercer Estado o a la organización internacional de que se trate ICUE originada en el Consejo en el ámbito de la política exterior y de seguridad común, tras haber obtenido el consentimiento del originador de todo material de origen contenido en ella. El Alto Representante podrá delegar tal autorización en altos funcionarios del SEAE o en los Representantes Especiales de la Unión.

39. Cuando exista un marco para el intercambio de información clasificada con un tercer Estado u organización internacional con arreglo a los puntos 2 o 3, se autorizará al Alto Representante a ceder ICUE, de conformidad con la decisión por la que se establezca la operación PCSD y respetando el principio del consentimiento previo del originador. El Alto Representante podrá delegar tal autorización en altos funcionarios del SEAE, en la Operación de la UE, en los Comandantes de la Fuerza o de la Misión, o en los Jefes de Misión de la UE.

▼B

Apéndices

Apéndice A

Definiciones

Apéndice B

Correspondencia de las clasificaciones de seguridad

Apéndice C

Lista de Autoridades Nacionales de Seguridad (ANS)

Apéndice D

Lista de abreviaturas

▼B

Apéndice A

DEFINICIONES

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

«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, de organización y de procedimiento.

«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.

«Autorización para acceder a ICUE»: una decisión de la autoridad facultada para proceder a los nombramientos de la SGC, adoptada sobre la base de una garantía concedida por una autoridad competente de un Estado miembro, que acredita que un funcionario u otro agente de la SGC o experto nacional destinado en la SGC en comisión de servicio puede tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada, siempre que se haya establecido su necesidad de conocer dicha información y haya sido adecuadamente informado sobre sus responsabilidades.

«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 y mantenimiento, y desmantelamiento.

«Contrato clasificado»: el contrato celebrado entre la SGC 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 dicha información.

«Subcontrato clasificado»: el contrato celebrado por un contratista de la SGC 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 dicha información.

«Sistema de información y comunicaciones» (SIC) — véase el artículo 10, apartado 2.

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

«Material de cifra»: algoritmos criptológicos, módulos criptológicos *software* y *hardware*, y productos, incluida la información sobre su uso y la documentación pertinente y los datos de claves.

«Producto criptológico»: producto que tiene como función primordial y principal la prestación de servicios de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, no repudio) mediante uno o varios mecanismos criptológicos.

▼B

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

«Desclasificación»: supresión de toda clasificación de seguridad.

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

«Autoridad de Seguridad Designada» (ASD): la autoridad responsable ante la Autoridad Nacional de Seguridad (ANS) de un Estado miembro, encargada de comunicar a las sociedades industriales u otro tipo de entidades la política nacional en 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.

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

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

«Información clasificada de la UE» (ICUE) — véase el artículo 2, apartado 1.

«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.

«Manejo» de ICUE: toda intervención posible a la que puede 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.

«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.

«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.

«Seguridad industrial» — véase el artículo 11, apartado 1.

«Garantía de la información» — véase el artículo 10, apartado 1.

«Interconexión» — véase el anexo IV, punto 32.

«Tratamiento de la información clasificada» — véase el artículo 9, apartado 1.

▼B

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

«Originador»: la institución, organismo o agencia de la Unión, el Estado miembro, el tercer Estado o la organización internacional bajo cuya autoridad se ha producido información clasificada o se ha introducido en las estructuras de la Unión.

«Seguridad en el personal» — véase el artículo 7, apartado 1.

«Habilitación personal de seguridad» (HPS): 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.

«Certificado de habilitación personal de seguridad» (CHPS): el certificado expedido por una autoridad competente mediante el cual se establece que una persona está habilitada y dispone de un certificado de habilitación de seguridad o una autorización válidos para acceder a ICUE expedidos por la autoridad facultada para proceder a los nombramientos, y que indica el grado de ICUE a que puede tener acceso (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), el período de validez de la habilitación y la fecha de caducidad del propio certificado.

«Seguridad física» — véase el artículo 8, apartado 1.

«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.

«Inscripción en un registro» — véase el anexo III, punto 18.

«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.

«Riesgo»: la posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades internas o externas de una organización o de cualquier sistema 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.

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

— «Evaluación del riesgo»: consiste en determinar las amenazas y las vulnerabilidades, y llevar a cabo el correspondiente análisis del riesgo, es decir, el análisis de la probabilidad y de las repercusiones.

— «Comunicación del riesgo»: consiste en sensibilizar de los riesgos a las comunidades de usuarios de SIC, informar de tales riesgos a las autoridades responsables de la aprobación y a las autoridades operativas.

▼B

— «Tratamiento del riesgo»: consiste en atenuar, suprimir o reducir el riesgo (adoptando una combinación adecuada de medidas técnicas, físicas, de gestión o de procedimiento), transferir el riesgo o hacer un seguimiento del mismo.

«Cláusula sobre aspectos de la seguridad»: conjunto de condiciones contractuales especiales impuestas por la autoridad contratante y que forman parte integrante de un contrato clasificado que conlleve el acceso a ICUE o la creación de ese tipo de información; en ella se enumeran los requisitos de seguridad o los elementos del contrato que requieren protección de seguridad.

«Guía de clasificación de seguridad»: 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.

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

«Modo de operación de seguridad»: el conjunto de las condiciones de funcionamiento de un SIC, definidas sobre la base de la clasificación de la información manejada y de los grados de habilitación, las aprobaciones formales de acceso y la necesidad de conocer de los usuarios. Existen cuatro modos de operación para el manejo y la transmisión de información clasificada: dedicado, unificado a nivel superior, compartimentado y multinivel.

— «Modo dedicado»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él y tienen la misma necesidad de conocer toda la información manejada en el SIC.

— «Modo unificado a nivel superior»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, pero en el que no todas las personas con acceso al SIC tienen la misma necesidad de conocer la información manejada en él; la aprobación para acceder a la información puede darla una persona.

— «Modo compartimentado»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, pero no todas las personas con acceso al SIC poseen una autorización formal de acceso a toda la información manejada en él; la autorización formal supone, a diferencia del acceso que se concede a discreción de una persona, la existencia de una gestión formal centralizada del control de acceso.

▼B

— «Modo multinivel»: modo de operación en el que no todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, y no todas las personas con acceso al SIC tienen la misma necesidad de conocer la información manejada en él.

«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 cualquiera de los sistemas que utiliza. Abarca todas las actividades relacionadas con los riesgos, incluida la evaluación, tratamiento, aceptación y comunicación.

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

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

«Vulnerabilidad»: una debilidad, cualquiera que sea su naturaleza, que pueda ser aprovechada por una o varias amenazas. La vulnerabilidad puede resultar de una omisión o guardar relación con una deficiencia en el grado, completitud o coherencia de los controles, y puede ser técnica, física, de procedimiento, de organización o de funcionamiento.

▼M1

Apéndice B

CORRESPONDENCIA DE LAS CLASIFICACIONES DE SEGURIDAD

UE | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU 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])*[infra]* |

Bulgaria | Строго секретно | Секретно | Поверително | За служебно ползване |

República Checa | Přísně tajné | Tajné | Důvěrné | Vyhrazené |

Dinamarca | YDERST HEMMELIGT | HEMMELIGT | FORTROLIGT | TIL TJENESTEBRUG |

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 Abr: ΑΑΠ | Απόρρητο Abr: (ΑΠ) | Εμπιστευτικό Abr: (ΕΜ) | Περιορισμένης Χρήσης Abr: (ΠΧ) |

España | SECRETO | RESERVADO | CONFIDENCIAL | DIFUSIÓN LIMITADA |

Francia | Très Secret Défense | Secret Défense | Confidentiel Défense | nota ([3]) infra |

Croacia | VRLO TAJNO | TAJNO | POVJERLJIVO | OGRANIČENO |

Italia | Segretissimo | Segreto | Riservatissimo | Riservato |

Chipre | Άκρως Απόρρητο Abr: (ΑΑΠ) | Απόρρητο Abr: (ΑΠ) | Εμπιστευτικό Abr: (ΕΜ) | Περιορισμένης Χρήσης Abr: (ΠΧ) |

Letonia | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |

Lituania | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |

([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]) 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.

▼M1

Luxemburgo | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |

Hungría | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |

Malta | L-Ogħla Segretezza | Sigriet | Kunfidenzjali | Ristrett |

Top Secret | Secret | Confidential | Restricted ([1])

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 | Secret de serviciu |

Eslovenia | STROGO TAJNO | TAJNO | ZAUPNO | INTERNO |

Eslovaquia | Prísne tajné | Tajné | Dôverné | Vyhradené |

Finlandia | ERITTÄIN SALAINEN YTTERST HEMLIG | SALAINEN HEMLIG | LUOTTAMUKSELLINEN KONFIDENTIELL | KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG |

Suecia ([2]) | HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET HEMLIG | HEMLIG/CONFIDENTIAL HEMLIG | HEMLIG/RESTRICTED HEMLIG |

Reino Unido | UK TOP SECRET | UK SECRET | nota ([3]) infra | UK OFFICIAL-SENSITIVE |

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

([2]) Suecia: Las marcas de clasificación de seguridad indicadas en la línea superior son utilizadas por las autoridades de defensa, y las indicadas en la línea inferior las utilizadas por otras autoridades.

([3]) El Reino Unido no utiliza ya la clasificación «UK CONFIDENTIAL» en su sistema nacional. El Reino Unido trata y protege la información clasificada «CONFIDENTIEL UE/EU CONFIDENTIAL» con arreglo a los requisitos de protección de seguridad correspondientes a «UK SECRET».

▼B

Apéndice C

LISTA DE AUTORIDADES NACIONALES DE SEGURIDAD (ANS)

BÉLGICA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. de la Secretaría: +32 25014542
Fax +32 25014596
Correo electrónico: nvo-ans@diplobel.fed.be

BULGARIA
State Commission on Information Security
90 Cherkovna Str.
1505 Sofía

Tel. +359 29333600
Fax +359 29873750
Correo electrónico: dksi@government.bg
Página web: www.dksi.bg

REPÚBLICA CHECA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel. +420 257283335
Fax +420 257283110
Correo electrónico: czech.nsa@nbu.cz
Página web: www.nbu.cz

DINAMARCA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel. +45 33325566
Fax +45 33931320

ESTONIA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel. +372 717 0019, +372 7170117
Fax +372 7170213
Correo electrónico: nsa@mod.gov.ee

IRLANDA
National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2

Tel. +353 14780822
Fax +353 14082959

GRECIA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff
(HNDGS)
Counter Intelligence and Security Directorate
(NSA)
227-231 HOLARGOS
STG 1020 ATHENS

Tel. +30 2106572045
+30 2106572009
Fax +30 2106536279
+30 2106577612

ESPAÑA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel. +34 913725000
Fax +34 913725808
Correo electrónico: nsa-sp@areatec.com

▼B

ALEMANIA Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel. +49 30186810 Fax +49 30186811441 Correo electrónico: oesIII3@bmi.bund.de	**FRANCIA** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200
CROACIA Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 www.uvns.hr	**LUXEMBURGO** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 central +352 24782253 direct Fax +352 24782243
ITALIA Presidenza del Consiglio dei Ministri D.I.S.-U.C.Se. Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Fax +39 064885273	**HUNGRÍA** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel. +36 (1) 7952303 Fax +36 (1) 7950344 Postal address: H-1357 Budapest, PO Box 2 Correo electrónico: nbf@nbf.hu Página web: www.nbf.hu
CHIPRE ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 Correo electrónico: cynsa@mod.gov.cy	**MALTA** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321
LETONIA National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 Fax +371 67025454 Correo electrónico: ndi@sab.gov.lv	**PAÍSES BAJOS** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522

▼B

LITUANIA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel. +370 706 66701, +370 706 66702 Fax +370 706 66700 Correo electrónico: nsa@vsd.lt	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel. +43 1531152594 Fax +43 1531152615 Correo electrónico: ISK@bka.gv.at
POLONIA Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857360 Fax +48 225858509 Correo electrónico: nsa@abw.gov.pl Página web: www.abw.gov.pl	**ESLOVAQUIA** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel. +421 268692314 Fax +421 263824005 Página web: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711	**FINLANDIA** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Teléfono 1: +358 160505890 Fax +358 916055140 Correo electrónico: NSA@formin.fi
RUMANÍA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mures nr. 4012275 Bucharest Tel. +40 212245830 Fax +40 212240714 Correo electrónico: nsa.romania@nsa.ro Página web: www.orniss.ro	**SUECIA** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S-103 39 Stockholm Tel. +46 84051000 Fax +46 87231176 Correo electrónico: ud-nsa@foreign.ministry.se
ESLOVENIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 Correo electrónico: gp.uvtp@gov.si	**REINO UNIDO** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Teléfono 1: +44 2072765645 Teléfono 2: +44 2072765497 Fax +44 2072765651 Correo electrónico: UK-NSA@cabinet-office.x.gsi.gov.uk

▼B

Apéndice D

LISTA DE ABREVIATURAS

Acrónimo	Significado
AAS	Autoridad de Acreditación de Seguridad
ACC	Autoridad de Certificación Criptológica
ADA	Autoridad debidamente acreditada
ADC	Autoridad de Distribución Criptológica
AGI	Autoridad de Garantía de la Información
ANS	Autoridad Nacional de Seguridad
ASD	Autoridad de Seguridad Designada
CCTV	Circuito cerrado de televisión
CHPS	Certificado de habilitación personal de seguridad
Coreper	Comité de Representantes Permanentes
ECSD	Dirección de Seguridad de la Comisión Europea
GI	Garantía de la Información
HPS	Habilitación personal de seguridad
ICUE	Información clasificada de la UE
PCSD	Política Común de Seguridad y Defensa
PESC	Política Exterior y de Seguridad Común
REUE	Representante Especial de la UE
SDI	Sistema de detección de intrusiones
SGC	Secretaría General del Consejo
SIC	Sistemas de información y comunicaciones que manejen ICUE
TI	Tecnologías de la información