DECISIÓN (UE, Euratom) 2015/444 DE LA COMISIÓN

de 13 de marzo de 2015

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

LA COMISIÓN EUROPEA,

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

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica y, en particular, su artículo 106,

Visto el Protocolo nº 7 sobre los privilegios y las inmunidades de la Unión Europea anejo a los Tratados y, en particular, su artículo 18,

Considerando lo siguiente:

(1) Las disposiciones de seguridad de la Comisión relativas a la protección de la información clasificada de la Unión Europea (ICUE) deben revisarse y actualizarse, teniendo en cuenta la evolución institucional, organizativa, operativa y tecnológica.

(2) La Comisión Europea ha suscrito instrumentos sobre cuestiones de seguridad para sus sedes principales con los gobiernos de Bélgica, Luxemburgo e Italia [1].

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

(4) Es importante que el Parlamento Europeo y las demás instituciones, órganos, organismos y 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.

(5) Los riesgos para la ICUE deberán gestionarse como un proceso. El objetivo de este proceso será determinar los riesgos conocidos para la seguridad, definir medidas de seguridad para reducir dichos riesgos a un nivel aceptable de conformidad con los principios básicos y normas mínimas establecidos en la presente Decisión, y aplicar estas medidas conforme al concepto de defensa en profundidad. La eficacia de dichas medidas será continuamente evaluada.

(6) Dentro de la Comisión, por seguridad física dirigida a la protección de la información clasificada se entenderá la aplicación de medidas de protección físicas y técnicas para impedir el acceso no autorizado a la ICUE.

(7) Por tratamiento de la ICUE 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 capítulos 2, 3 y 5 de la presente Decisión y contribuyan, así, a disuadir, descubrir y subsanar cualquier acto deliberado o accidental que pueda comprometer o suponer la pérdida de dicha información. Estas medidas se refieren, en particular, a la producción, almacenamiento, registro, copia, traducción, recalificación, desclasificación, traslado y destrucción de ICUE y complementan las normas generales sobre gestión de documentos de la Comisión [Decisiones 2002/47/CE, CECA, Euratom [2] y 2004/563/CE, Euratom [3]].

---

[1] Véase el «Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité» de 31 de diciembre de 2004, el «Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois», de 20 de enero de 2007, y el «Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale», de 22 de julio de 1959.

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

[3] Decisión 2004/563/CE, Euratom de la Comisión, de 7 de julio de 2004, por la que se modifica su Reglamento interno (DO L 251 de 27.7.2004, p. 9).

(8) Las disposiciones de la presente Directiva no afectarán a:

a) Reglamento (Euratom) nº 3 ([1]);

b) Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo ([2]);

c) Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo ([3]);

d) Reglamento (CEE, Euratom) nº 354/83 del Consejo ([4]).

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO 1

PRINCIPIOS BÁSICOS Y ESTÁNDARES MÍNIMOS

Artículo 1

Definiciones

A efectos de la presente Decisión, se entenderá por:

1) «Servicio de la Comisión»: toda Dirección General o servicio de la Comisión, o cualquier gabinete de un miembro de la Comisión.

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

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

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

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

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

7) «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, registro, tratamiento, traslado, reducción del grado de clasificación, desclasificación y destrucción. En relación con los sistemas de información y comunicaciones (SIC) abarca asimismo su recopilación, exposición, transmisión y almacenamiento.

8) «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.

9) «Normas de desarrollo»: todo conjunto de normas o directrices de seguridad adoptado de conformidad con el capítulo 5 de la Decisión (EU, Euratom) 2015/443 de la Comisión ([5]).

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

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

12) «Locales»: todo inmueble o propiedad y posesiones asimiladas de la Comisión.

([1]) Reglamento (Euratom) nº 3, de 31 de julio de 1958, relativo a la aplicación del artículo 24 del Tratado constitutivo de la Comunidad Europea de la Energía Atómica (DO 17 de 6.10.1958, p. 406/58).

([2]) Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

([3]) Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

([4]) Reglamento (CEE, Euratom, CECA) nº 354/83 del Consejo, de 1 de febrero de 1983, relativo a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía Atómica (DO L 43 de 15.2.1983, p. 1).

([5]) Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (véase la página 41 del presente Diario Oficial).

13) «Proceso de gestión de riesgos de seguridad»: 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.

14) «Estatuto de los funcionarios»: Estatuto de los funcionarios de la Unión Europea y Régimen aplicable a otros agentes de la Unión Europea establecido mediante el Reglamento (CEE, Euratom, CECA) nº 259/68 del Consejo ([1]).

15) «Amenaza»: 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.

16) «Vulnerabilidad»: 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.

Artículo 2

Objeto y ámbito de aplicación

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

3. Sin perjuicio de las indicaciones específicas relativas a grupos concretos de personal, la presente Decisión se aplicará a los miembros de la Comisión, al personal de la Comisión incluido en el ámbito de aplicación del Estatuto de los funcionarios y de las condiciones de empleo de otros agentes de las Comunidades Europeas, a los expertos nacionales enviados en comisión de servicio a la Comisión (en lo sucesivo, «expertos nacionales en comisión de servicios»), a los proveedores de servicios y su personal, a los trabajadores en prácticas y a cualquier persona con acceso a los edificios de la Comisión u otros activos, o a la información manejada por la Comisión.

4. Las disposiciones de la presente Decisión se entenderán sin perjuicio de lo dispuesto en la Decisión 2002/47/CE, CECA, Euratom y la Decisión 2004/563/CE, Euratom.

Artículo 3

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) TRES 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;

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 Europea 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 que no sean marcas de clasificación, sino que se destinen a 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.

([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).

Artículo 4

Gestión de la clasificación

1. Cada uno de los miembros de la Comisión o de los servicios de la Comisión se asegurarán de que la ICUE que crean se clasifique adecuadamente, quede claramente marcada como ICUE y solo conserve su grado de clasificación mientras sea necesario.

2. Sin perjuicio de lo dispuesto en el artículo 26, no se podrá rebajar el grado de clasificación de la ICUE ni desclasificarla, ni modificar o suprimir las marcas de clasificación de seguridad a que se refiere el artículo 3, apartado 2, sin el consentimiento previo por escrito del originador.

3. En su caso, se adoptarán normas de desarrollo para el manejo de la ICUE, que incluirán una guía práctica de clasificación, de conformidad con el artículo 60.

Artículo 5

Protección de la información clasificada

1. La ICUE se protegerá de conformidad con la presente Decisión y sus normas de desarrollo.

2. El poseedor de cualquier ICUE tendrá la responsabilidad de protegerla de conformidad con la presente Decisión y sus normas de desarrollo, con arreglo a las normas previstas en el capítulo 4.

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

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.

Artículo 6

Gestión del riesgo de seguridad

1. 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 la que se conserve, y la amenaza de actividades maliciosas o delictivas, evaluadas localmente, en particular el espionaje, el sabotaje y el terrorismo.

2. 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.

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

Artículo 7

Aplicación de la presente Decisión

1. En caso necesario, se adoptarán normas de desarrollo que completen o faciliten la aplicación de la presente Decisión, con arreglo a lo dispuesto en el artículo 60.

2. Los servicios de la Comisión adoptarán todas las medidas necesarias que sean de su competencia con el fin de garantizar que, cuando manejen o almacenen ICUE o cualquier otra información clasificada, se apliquen la presente Decisión y las normas de desarrollo correspondientes.

3. Las medidas de seguridad adoptadas en aplicación de la presente Decisión deberán ajustarse a los principios de seguridad de la Comisión establecidos en el artículo 3 de la Decisión (UE, Euratom) 2015/443.

4. El director general de la Dirección General de Recursos Humanos y Seguridad establecerá la autoridad de seguridad de la Comisión en el seno de la Dirección General de Recursos Humanos y Seguridad. La autoridad de seguridad de la Comisión dispondrá de las competencias que le sean asignadas por la presente Decisión y sus normas de desarrollo.

5. En cada servicio de la Comisión, el responsable local de Seguridad (LSO), tal como se contempla en el artículo 20 de la Decisión (UE, Euratom) 2015/443, tendrá las siguientes responsabilidades generales en materia de protección de la ICUE conforme a lo dispuesto en la presente Decisión, en estrecha cooperación con la Dirección General de Recursos Humanos y Seguridad:

a) gestión de las solicitudes de autorizaciones de seguridad para el personal;

b) contribución a la formación en materia de seguridad y sesiones de información sobre sensibilización;

c) supervisión del controlador del registro (RCO) del servicio;

d) información sobre fallos de seguridad y comprometimiento de la ICUE;

e) custodia de llaves de repuesto y registro escrito de cada combinación;

f) asunción de otras tareas relacionadas con la protección de la ICUE o establecidas por las normas de desarrollo.

Artículo 8

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 y sus normas de desarrollo.

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 de la Comisión.

4. Cuando se tenga conocimiento o sospechas fundadas de que una ICUE se ha visto comprometida o se ha perdido, se realizará una investigación de seguridad con arreglo a lo dispuesto en el artículo 13 de la Decisión (UE, Euratom) 2015/443.

5. Se tomarán todas las medidas adecuadas 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.

6. 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 el Estatuto de los funcionarios. 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.

CAPÍTULO 2

SEGURIDAD EN EL PERSONAL

Artículo 9

Definiciones

A los efectos del presente capítulo, se entenderá por:

1) «Autorización para acceder a ICUE»: decisión de la autoridad de seguridad de la Comisión, 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 Comisión o experto nacional destinado en la Comisión 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. De la persona que se ajuste a esta descripción se dirá que tiene «autorización de seguridad».

2) «Autorización personal de seguridad»: aplicación de medidas que garanticen que el acceso a la ICUE se concede únicamente a personas que:

   a) tengan necesidad de conocer;

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

   c) hayan sido instruidas sobre sus responsabilidades.

3) «Habilitación personal de seguridad» (HPS): 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, siempre que se haya determinado su «necesidad de conocer» y haya sido adecuadamente informada de sus responsabilidades, tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada.

4) «Certificado de habilitación personal de seguridad» (CHPS): certificado expedido por una autoridad competente mediante el cual se establece que una persona dispone de un certificado de habilitación de seguridad o una autorización válidos para acceder a ICUE expedidos por la autoridad de seguridad de la Comisión, 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.

5) «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 habilitación de seguridad para acceder a ICUE de un determinado nivel (CONFIDENTIEL UE/EU CONFIDENTIAL o superior).

Artículo 10

Principios básicos

1. Solo se concederá acceso a ICUE a aquella persona:

1) cuya necesidad de conocer se haya determinado;

2) que haya sido instruida sobre las normas de seguridad para la protección de la ICUE y las correspondientes directrices y estándares de seguridad, y que haya aceptado sus responsabilidades en lo que respecta a la protección de dicha información;

3) en el caso de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior: a quien se haya concedido una habilitación 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.

2. Todas las personas cuyas funciones puedan requerir el acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior deberán haber sido habilitadas para el grado correspondiente antes de poder acceder a dicha información. La persona de que se trate dará su consentimiento por escrito para ser sometida al procedimiento de habilitación de seguridad. De no hacerlo, se entenderá que el interesado no puede ser destinado a un puesto de trabajo, función o misión que implique el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior.

3. 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.

4. 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 realizada por las autoridades competentes de un Estado miembro, de conformidad con sus disposiciones legales y reglamentarias nacionales.

5. La autoridad de seguridad de la Comisión será la única responsable de la coordinación con las autoridades nacionales de seguridad (ANS) u otras autoridades nacionales competentes en el contexto de todas las cuestiones relacionadas con la habilitación de seguridad. Todos los contactos entre los servicios de la Comisión y su personal y las ANS y otras autoridades competentes se efectuarán a través de la autoridad de seguridad de la Comisión.

Artículo 11

Procedimiento de autorización de seguridad

1. Cada director general o jefe de servicio de la Comisión determinará los puestos dentro de sus servicios cuyos titulares deben tener acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior para cumplir sus obligaciones en materia de seguridad y deben, por tanto, ser autorizados.

2. En cuanto tenga conocimiento de que una persona será nombrada para un puesto que requiera acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, el LSO del servicio de la Comisión de que se trate informará a la autoridad de seguridad de la Comisión, que remitirá a la persona el cuestionario de habilitación de seguridad emitido por la ANS del Estado miembro en virtud de cuya nacionalidad la persona haya sido nombrada miembro del personal de las instituciones europeas. El interesado deberá dar su consentimiento por escrito para ser sometido al procedimiento de habilitación de seguridad y enviará el cuestionario debidamente cumplimentado en el plazo más breve a la autoridad de seguridad de la Comisión.

3. La autoridad de seguridad de la Comisión remitirá el cuestionario de habilitación de seguridad cumplimentado a la ANS del Estado miembro en virtud de cuya nacionalidad la persona haya sido nombrada miembro del personal de las instituciones europeas, solicitando que se lleve a cabo una investigación de seguridad para el nivel de la ICUE a que el interesado requerirá acceso.

4. En los casos en que la autoridad de seguridad de la Comisión tenga información pertinente para una investigación de seguridad sobre una persona que ha solicitado una habilitación de seguridad, la autoridad de seguridad de la Comisión, con arreglo a las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS competente.

5. Una vez concluida la investigación de seguridad, y tan pronto como sea posible después de haber sido notificada por la ANS pertinente acerca de su evaluación general de las conclusiones de dicha investigación, la autoridad de seguridad de la Comisión:

a) podrá conceder una autorización de acceso a la ICUE a la persona de que se trate y autorizar el acceso a la ICUE del grado pertinente hasta una fecha que especifique, pero para un período máximo de 5 años, en caso de que la investigación de seguridad permita garantizar que no se conoce ningún dato desfavorable que ponga en entredicho la lealtad, honradez y fiabilidad de la persona;

b) en caso de que la investigación de seguridad no permita dar semejante garantía, de conformidad con las disposiciones legales y reglamentarias pertinentes, lo notificará a la persona, que podrá requerir ser oída por la autoridad de seguridad de la Comisión, quien, a su vez, podrá pedir a la ANS competente cuantas aclaraciones le pueda facilitar, de conformidad con sus disposiciones legales y reglamentarias nacionales. En caso de que el resultado de la investigación de seguridad se confirme, no se expedirá la autorización de acceso a la ICUE.

6. 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 de seguridad de la Comisión de acuerdo con lo dispuesto en el Estatuto de los funcionarios.

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

8. En caso de que el período de servicio de la persona no haya comenzado al término de 12 meses a partir de la notificación del resultado de la investigación de seguridad a la autoridad de seguridad de la Comisión, o en caso de que haya una interrupción de 12 meses en el tiempo de servicio de esa misma persona durante el cual no haya estado empleada en la Comisión ni en otra institución, órgano u organismo de la Unión, ni en una administración nacional de un Estado miembro, la autoridad de seguridad de la Comisión remitirá el asunto a la ANS correspondiente para que confirme que sigue siendo válido y adecuado.

9. Si la autoridad de seguridad de la Comisión tuviera conocimiento de que una persona que tiene autorización para acceder a ICUE representa un riesgo para la seguridad, la autoridad de seguridad de la Comisión, con arreglo a las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS correspondiente.

10. Si una ANS notifica a la autoridad de seguridad de la Comisión la retirada de una garantía concedida de conformidad con el apartado 5, letra a), a una persona que tiene autorización de acceso a ICUE, la autoridad de seguridad de la Comisión 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 ICUE y de los puestos en los que pudiera tener acceso a dicha información o poner en peligro la seguridad.

11. La decisión de retirar o suspender una autorización de acceso a ICUE a una persona que entre en el ámbito de aplicación de la presente Decisión, y, en su caso, los motivos para hacerlo, se comunicarán a la persona, que podrá requerir ser oída por la autoridad de seguridad de la Comisión. La información facilitada por la ANS deberá ajustarse a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión. Se podrá apelar contra las decisiones de la autoridad seguridad de la Comisión de acuerdo con lo dispuesto en el Estatuto de los funcionarios.

12. Los servicios de la Comisión deberán asegurarse de que los expertos nacionales en comisión de servicio para un puesto que requiera autorización de seguridad para acceder a ICUE presenten, antes de asumir sus funciones, una HPS o un Certificado de Habilitación Personal de Seguridad (CHPS) válidos, de conformidad con la normativa y la legislación nacional, a la autoridad de seguridad de la Comisión que, basándose en ello, expedirá una autorización para acceder a ICUE hasta el nivel equivalente a aquel a que se refiere la habilitación nacional de seguridad, con una validez máxima igual al período de la misión.

Acceso a ICUE de personas debidamente autorizadas en virtud de sus funciones

13. Los miembros de la Comisión, que tengan acceso a ICUE en virtud de sus funciones sobre la base del Tratado, serán informados de sus obligaciones respecto de la protección de la ICUE.

Habilitaciones de seguridad y registros de la autorización de seguridad

14. La autoridad de seguridad de la Comisión conservará registros de las habilitaciones de seguridad y de las autorizaciones concedidas para acceder a ICUE, de conformidad con lo dispuesto en la presente Decisión. Estos registros indicarán, como mínimo, el nivel de ICUE al que el interesado puede tener acceso, la fecha de concesión de la habilitación de seguridad y su período de validez.

15. La autoridad de seguridad de la Comisión 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 autorización para acceder a la ICUE de que se trate y la fecha de caducidad del propio certificado.

Renovación de las autorizaciones de seguridad

16. Tras la concesión inicial de una autorización de seguridad, y siempre que la persona haya prestado servicio de forma ininterrumpida en la Comisión Europea u otra institución, órgano u organismo de la Unión y siga necesitando acceder a ICUE, la autorización de seguridad se revisará con vistas a su renovación, con carácter general, cada 5 años a partir de la fecha de notificación del resultado de la última investigación de seguridad que haya servido de base para dicha autorización.

17. La autoridad de seguridad de la Comisión podrá prorrogar la validez de la autorización de seguridad vigente por un período de hasta 12 meses, si no se ha recibido información desfavorable de la ANS pertinente o de otra autoridad nacional competente en un plazo de 2 meses a partir de la fecha de envío de la solicitud de renovación y del correspondiente cuestionario de habilitación de seguridad. Si al término de este período de 12 meses, la ANS pertinente u otro organismo nacional competente no ha comunicado a la autoridad de seguridad de la Comisión su dictamen, la persona solo podrá desempeñar funciones que no requieran una habilitación de seguridad.

Artículo 12

Sesiones informativas en materia de autorización de seguridad

1. Tras participar en la sesión informativa en materia de autorización de seguridad organizada por la autoridad de seguridad de la Comisión, todas las personas que hayan recibido una autorización de seguridad reconocerán por escrito que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias del comprometimiento de esta información. La autoridad de seguridad de la Comisión llevará un registro de estas declaraciones escritas.

2. 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 la autoridad de seguridad de la Comisión de cualquier actitud o actividad que consideren sospechosa o inusual.

3. 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.

Artículo 13

Autorizaciones de seguridad temporales

1. En circunstancias excepcionales, cuando esté debidamente justificado en interés del servicio y en espera de la conclusión de una investigación de seguridad completa, la autoridad de seguridad de la Comisión podrá conceder 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, sin perjuicio de las disposiciones relativas a la renovación de las habilitaciones de seguridad. La validez de estas autorizaciones temporales no será superior a 6 meses ni permitirá acceder a información clasificada de grado TRÈS SECRET UE/EU TOP SECRET.

2. Tras haber sido informadas de conformidad con el artículo 12, apartado 1, todas las personas a las que se haya concedido una 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 autoridad de seguridad de la Comisión llevará un registro de estas declaraciones escritas.

Artículo 14

Asistencia a reuniones clasificadas organizadas por la Comisión

1. Los servicios de la Comisión responsables de la organización de reuniones en las que se examinará información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, a través de su LSO o a través del organizador de la reunión, informarán a la autoridad de seguridad de la Comisión con mucha antelación de las fechas, horarios, lugar y participantes en dichas reuniones.

2. Sin perjuicio de las disposiciones del artículo 11, apartado 13, las personas que deban participar en reuniones organizadas por la Comisión 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 o autorización de seguridad. Se denegará el acceso a este tipo de reuniones confidenciales a las personas para las que la autoridad de seguridad de la Comisión no haya comprobado la existencia de un CHSP u otra prueba de habilitación de seguridad, o a participantes de la Comisión que no posean una autorización de seguridad.

3. Antes de organizar una reunión clasificada, el organizador de la reunión o el LSO del servicio de la Comisión que haya organizado la reunión solicitará a los participantes externos que proporcionen a la autoridad de seguridad de la Comisión un CHSP u otra prueba de habilitación de seguridad. La autoridad de seguridad de la Comisión informará al LSO o al organizador de la reunión acerca de los CHSP u otra prueba de HPS recibidos. Cuando proceda, podrá utilizarse una lista recapitulativa de nombres en la que figuren las pruebas pertinentes de su habilitación de seguridad.

4. En caso de que la autoridad de seguridad de la Comisión sea informada por las autoridades competentes de que se ha retirado la HPS a una persona cuyas funciones requieran la asistencia a reuniones organizadas por la Comisión, la autoridad de seguridad de la Comisión deberá informar de inmediato al LSO del servicio de la Comisión responsable de la organización de la reunión.

Artículo 15

Acceso potencial a ICUE

Los correos, agentes de seguridad y escoltas serán debidamente autorizados 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.

CAPÍTULO 3

SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

Artículo 16

Principios básicos

1. 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 de riesgos, de conformidad con la presente Decisión y sus normas de desarrollo.

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

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

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

c) disuadiendo, impidiendo y detectando actividades no autorizadas, e

d) impidiendo o retrasando la entrada subrepticia o por la fuerza de intrusos.

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 capítulo 5.

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 presente capítulo, y serán aprobadas por la autoridad de seguridad de la Comisión.

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

Artículo 17

Requisitos y medidas de seguridad física

1. Las medidas de seguridad física aplicables se determinarán sobre la base de una evaluación de las amenazas realizada por la autoridad de seguridad de la Comisión, si procede en consulta con otros servicios de la Comisión, otras instituciones, órganos u organismos de la Unión o autoridades competentes de los Estados miembros. La Comisión aplicará un proceso de gestión de riesgos para proteger la ICUE en sus locales, de modo que se garantice un grado de protección física acorde con el riesgo evaluado. El proceso de gestión de riesgos 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 instituciones, órganos u organismos, o los Estados miembros, como el sabotaje, el terrorismo, la subversión u otras actividades delictivas.

2. Al aplicar el concepto de defensa en profundidad, la autoridad de seguridad de la Comisión determinará la combinación apropiada de las medidas de seguridad física que deben aplicarse. A tal efecto, elaborará estándares, normas y criterios mínimos establecidos en las normas de desarrollo.

3. Podrá autorizarse a la autoridad de seguridad de la Comisión a llevar a cabo, en las entradas y salidas, registros que disuadan de todo intento no autorizado de introducir material en los locales o edificios o de sacar de ellos ICUE.

4. Cuando exista el riesgo de que una ICUE sea objeto de miradas indiscretas, incluso accidentalmente, los servicios de la Comisión tomarán medidas adecuadas, definidas por la autoridad de seguridad de la Comisión, para contrarrestar ese riesgo.

5. Para los nuevos establecimientos, los requisitos de seguridad física y sus especificaciones funcionales se definirán de acuerdo con la autoridad de seguridad de la Comisión como parte de la planificación y el diseño de los mismos. Para los establecimientos ya existentes, los requisitos de seguridad física se aplicarán de conformidad con los estándares, normas y criterios mínimos establecidos en las normas de desarrollo.

Artículo 18

Equipo para la protección física de la ICUE

1. Para la protección física de la ICUE se establecerán dos tipos de zonas físicamente protegidas:

a) zonas administrativas, y

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

2. La Autoridad de Acreditación de Seguridad de la Comisión decidirá si una zona cumple los requisitos para ser designada zona administrativa, zona de acceso restringido o zona de acceso restringido protegida por medios técnicos.

3. Para las zonas administrativas:

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

b) solo se permitirá el acceso sin acompañamiento a las personas debidamente autorizadas por la autoridad de seguridad de la Comisión o cualquier otra autoridad competente, y

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

4. 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;

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

5. 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.

6. 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 («SDI»), 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 el artículo 20;

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

c) estas zonas serán objeto de inspecciones físicas o técnicas regularmente por la autoridad de seguridad de la Comisión; además, serán inspeccionadas también cada vez 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.

7. No obstante lo dispuesto en el punto 6, letra d), todos los equipos de comunicaciones y todos los aparatos eléctricos o electrónicos deberán ser examinados por la autoridad de seguridad de la Comisión 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.

8. 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.

9. 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.

10. El LSO del servicio de la Comisión de que se trate definirá procedimientos operativos de seguridad para cada zona de acceso restringido bajo su responsabilidad en los que se disponga lo siguiente, de conformidad con las disposiciones de la presente Decisión y de sus normas de desarrollo:

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 autorización 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;

e) cualquier otra medida o procedimiento pertinente.

11. 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 de la Comisión y ofrecer una protección equivalente a la de un contenedor de seguridad aprobado para el almacenamiento de ICUE del mismo grado de clasificación.

Artículo 19

Medidas de protección física para el manejo y almacenamiento de la ICUE

1. La ICUE de grado RESTREINT UE/EU RESTRICTED se podrá manejar:

a) en una zona de acceso restringido;

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

c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la ICUE de conformidad con el artículo 31 y se haya comprometido a cumplir las medidas compensatorias establecidas en las normas de desarrollo, para garantizar que la ICUE está protegida del acceso de personas no autorizadas.

2. 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 normas de desarrollo.

3. 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) se haya comprometido a cumplir las medidas compensatorias establecidas en las normas de desarrollo para garantizar que el acceso a la ICUE se impide a personas no autorizadas,

   ii) mantenga la ICUE en todo momento bajo su control personal, y

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

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

5. La ICUE de nivel TRES SECRET UE/EU TOP SECRET se manejará en una zona de acceso restringido, establecida y mantenida por la autoridad de seguridad de la Comisión, y acreditada a dicho nivel por la Autoridad de Acreditación de Seguridad de la Comisión.

6. La ICUE de nivel TRES SECRET UE/EU TOP SECRET se almacenará en una zona de acceso restringido, a ese nivel, acreditada a dicho nivel por la Autoridad de Acreditación de Seguridad de la Comisión, en una de las condiciones siguientes:

a) En un contenedor de seguridad conforme a lo dispuesto en el artículo 18, con al menos uno de los controles adicionales siguientes:

   1) protección continua o verificación periódica por personal de seguridad o de servicio habilitado;

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

   o

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

Artículo 20

Gestión de llaves y combinaciones empleadas para la protección de ICUE

1. Los procedimientos de gestión de las llaves y combinaciones de las oficinas, salas, cámaras acorazadas y contenedores de seguridad se fijarán en las normas de desarrollo de conformidad con el artículo 60. Estos procedimientos deberán evitar accesos no autorizados.

2. 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.

CAPÍTULO 4

TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA DE LA UE

Artículo 21

Principios básicos

1. Todos los documentos de ICUE deben tratarse con arreglo a la política de la Comisión en materia de gestión de documentos y, en consecuencia, deben registrarse, clasificarse, conservarse y, por último, eliminarse, someterse a muestreo o trasladarse a los archivos históricos de conformidad con la lista común de conservación de expedientes de la Comisión Europea.

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. La información clasificada de grado TRÈS SECRET UE/EU TOP SECRET se inscribirá en registros especiales.

3. En el seno de la Comisión, se establecerá un sistema de registro de la ICUE de conformidad con lo dispuesto en el artículo 27.

4. Los servicios y locales de la Comisión en los que se maneje o almacene ICUE serán inspeccionados periódicamente por la autoridad de seguridad de la Comisión.

5. 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 capítulo 5;

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 capítulo 5, o

   ii) en los demás casos, según lo dispuesto en las normas de desarrollo.

Artículo 22

Clasificaciones y marcas

1. La información se clasificará cuando requiera protección respecto de su confidencialidad, de conformidad con lo dispuesto en el artículo 3, apartado 1.

2. El originador de la ICUE será responsable de determinar el grado de clasificación de seguridad atendiendo a las correspondientes normas de desarrollo, normas y directrices en materia de clasificación, y de la difusión inicial de la información.

3. El nivel de clasificación de la ICUE se determinará de conformidad con el artículo 3, apartado 2, y con las normas de desarrollo pertinentes.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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

Artículo 23

Marcas

Junto con una de las marcas de la clasificación de seguridad fijadas en el artículo 3, 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;

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

Artículo 24

Marcas abreviadas de clasificación

1. 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.

2. 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:

TRES 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

Artículo 25

Producción de ICUE

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

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

b) cada página irá numerada;

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

d) el documento estará fechado;

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

2. Cuando no sea posible aplicar el punto 1 a una ICUE, se tomarán otras medidas adecuadas de conformidad con las normas de desarrollo.

Artículo 26

Reducción del grado de clasificación y desclasificación de la ICUE

1. En el momento de producir la información, el originador indicará, cuando sea posible, si el grado de clasificación de la ICUE puede ser reducido o desclasificado a partir de una determinada fecha o tras un acontecimiento concreto.

2. Cada servicio de la Comisión revisará periódicamente la ICUE que haya generado para verificar si el grado de clasificación asignado sigue siendo aplicable. Las normas de desarrollo establecerán un sistema para revisar, con una frecuencia mínima quinquenal, el grado de clasificación de la ICUE que se haya generado en la Comisión. 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.

3. La información clasificada de grado RESTREINT UE/EU RESTRICTED originaria de la Comisión se considerará automáticamente desclasificada después de 30 años, de conformidad con lo dispuesto en el Reglamento (CEE, Euratom) nº 354/83, modificado por el Reglamento (CE, Euratom) nº 1700/2003 del Consejo ([1]).

Artículo 27

Sistema de registro de la ICUE en la Comisión

1. Sin perjuicio de lo dispuesto en el artículo 52, apartado 5, en cada servicio de la Comisión donde se maneje o almacene ICUE de nivel CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, se identificará un responsable local de registro de ICUE para garantizar que la ICUE se maneje de conformidad con las disposiciones de la presente Decisión.

2. El registro de ICUE gestionado por la Secretaría General será el registro central de ICUE de la Comisión, que actuará como:

— registro local de ICUE para la Secretaría General de la Comisión,

— registro de ICUE para los gabinetes de los miembros de la Comisión, a menos que estos hayan designado un registro local de ICUE,

— registro de ICUE para direcciones generales o servicios que no dispongan de un registro local de ICUE,

— punto principal de entrada y salida de toda la información clasificada de grado RESTREINT UE/EU RESTRICTED y hasta SECRET UE/EU SECRET inclusive, intercambiada entre la Comisión y sus servicios y terceros Estados y organizaciones internacionales, así como, cuando esté previsto en disposiciones específicas, para otras instituciones, órganos u organismos de la Unión.

3. En el seno de la Comisión, la autoridad de seguridad de la Comisión designará un registro para que actúe como principal organismo receptor y emisor de la información clasificada de grado TRES SECRET UE/EU TOP SECRET. Cuando proceda, podrán designarse registros secundarios para manejar dicha información.

4. 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.

5. Los registros de ICUE se constituirán como zonas de acceso restringido, según lo definido en el capítulo 3, y acreditados por la Autoridad de Acreditación de Seguridad (AAS).

Artículo 28

Controlador del registro

1. Cada registro de ICUE será gestionado por un controlador del registro («RCO»).

2. Los RCO deberán tener la debida habilitación de seguridad.

3. Los RCO estarán sujetos a la supervisión del LSO en los servicios de la Comisión por lo que respecta a la aplicación de las disposiciones sobre el tratamiento de los documentos de ICUE y el cumplimiento de las normas, estándares y directrices de seguridad pertinentes.

4. En el ámbito de su responsabilidad de gestionar el registro de ICUE al que haya sido asignado, el RCO deberá asumir las siguientes tareas de conformidad con lo dispuesto en la presente Decisión y en las correspondientes normas de desarrollo, estándares y directrices:

— gestionar las operaciones relativas al registro, conservación, reproducción, traducción, envío y destrucción, o traslado al servicio de archivos históricos de la ICUE,

— comprobar periódicamente la necesidad de mantener la clasificación de la información,

— asumir las demás tareas relacionadas con la protección de la ICUE definidas en las normas de desarrollo.

Artículo 29

Registro de la ICUE a efectos de seguridad

1. A efectos de la presente Decisión, por registro a efectos de seguridad (en lo sucesivo denominado «registro») se entenderá la aplicación de procedimientos que registren el ciclo de vida de la ICUE, incluida su difusión.

([1]) Reglamento (CE, Euratom) nº 1700/2003 del Consejo, de 22 de septiembre de 2003, por el que se modifica el Reglamento (CEE, Euratom) nº 354/83 relativo a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía Atómica (DO L 243 de 27.9.2003, p. 1).

2. Toda la información o el material clasificado de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior se inscribirá en registros especiales a su recepción o envío de una entidad organizativa.

3. Cuando se maneje o almacene ICUE utilizando un sistema de información y comunicación (SIC), los procedimientos de registro podrán llevarse a cabo mediante procesos dentro del propio SIC.

4. En las normas de desarrollo se establecerán disposiciones más detalladas sobre el registro de ICUE a efectos de seguridad.

Artículo 30

Copia y traducción de documentos clasificados de la UE

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

2. 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.

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

Artículo 31

Transporte de ICUE

1. La ICUE se transportará de forma que esté protegida frente a la divulgación no autorizada durante su transporte.

2. El transporte de ICUE estará sujeto a medidas de protección que deberán:

— ser acordes con el nivel de clasificación de la ICUE transportada,

— estar adaptadas a las condiciones específicas de su transporte, especialmente en función de si la ICUE se transporta:

  — dentro de un edificio o de un grupo independiente de edificios de la Comisión,

  — entre edificios de la Comisión situados en el mismo Estado miembro;

  — dentro de la Unión,

  — desde la Unión al territorio de un tercer Estado, y

  — estar adaptadas a la naturaleza y forma de la ICUE.

3. Dichas medidas de protección se establecerán en detalle en las normas de desarrollo o, en el caso de los proyectos y programas a que se refiere el artículo 42, como parte integrante de las instrucciones de seguridad de un programa o proyecto.

4. Las normas de desarrollo o las instrucciones de seguridad de un programa o proyecto deberán incluir disposiciones en relación con el nivel de la ICUE, por lo que se refiere a:

— el tipo de transporte, tal como transporte en mano, correo diplomático o militar, transporte por servicios postales o servicios de mensajería comercial,

— el empaquetado de la ICUE,

— contramedidas técnicas para la ICUE que se transporte por medios electrónicos,

— cualquier otra medida de procedimiento, física o electrónica,

— procedimientos de registro,

— el recurso a personal de seguridad autorizado.

5. Cuando se transmita ICUE por medios electrónicos, y no obstante lo dispuesto en el artículo 21, apartado 5, las medidas de protección establecidas en las normas de desarrollo pertinentes se completarán con las debidas contramedidas técnicas aprobadas por la autoridad de seguridad de la Comisión a fin de reducir al mínimo el riesgo de pérdida o comprometimiento.

Artículo 32

Destrucción de ICUE

1. Los documentos clasificados de la UE que hayan dejado de ser necesarios podrán destruirse, teniendo en cuenta las normas sobre archivos y las normas y reglamentos de la Comisión en materia de gestión de documentos y archivo, y en particular la lista común de conservación de la Comisión.

2. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior será destruida por el RCO del registro responsable de la ICUE por orden de su poseedor o de una autoridad competente. El RCO deberá actualizar en consecuencia los libros de registro y cualquier información relacionada con el registro.

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

4. 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 RCO del registro responsable de la ICUE conservará los certificados de destrucción de los documentos de grado TRES SECRET UE/EU TOP SECRET durante un período de 10 años como mínimo, y de los documentos con clasificación CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante 5 años como mínimo.

5. Los documentos clasificados, incluidos los de nivel RESTREINT UE/EU RESTRICTED, se destruirán por métodos que se definirán en las normas de desarrollo y que cumplirán las normas de la Unión pertinentes o normas equivalentes.

6. Los soportes de almacenamiento informático utilizados para la ICUE se destruirán con arreglo a procedimientos establecidos en las normas de desarrollo.

Artículo 33

Destrucción de ICUE en situaciones de urgencia

1. Los servicios de la Comisión que tengan EUCI prepararán planes basados en las condiciones locales para proteger el material clasificado de la UE en situaciones de crisis, incluidos, si fuera necesario, planes de destrucción y evacuación de urgencia. Promulgarán las instrucciones que se estimen necesarias para impedir que la ICUE caiga en manos de personas no autorizadas.

2. Las disposiciones para la salvaguardia o la destrucción de material CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET en una crisis no afectarán en ningún caso a la salvaguardia o destrucción de material TRÈS SECRET UE/EU TOP SECRET, incluido el equipo de mensajes cifrados, cuyo tratamiento debe tener prioridad sobre todas las demás tareas.

3. En caso de urgencia, 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 urgencia de la ICUE registrada.

4. En las normas de desarrollo se establecerán disposiciones más detalladas para la destrucción de ICUE.

CAPÍTULO 5

PROTECCIÓN DE INFORMACIÓN CLASIFICADA DE LA UE EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (SIC)

Artículo 34

Principios básicos de garantía de la información

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.

2. Una GI efectiva habrá de garantizar unos niveles apropiados de:

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.

3. La GI se basará en un proceso de gestión de riesgos.

Artículo 35

Definiciones

A efectos del presente capítulo, se entenderá por:

a) «Acreditación»: autorización formal y aprobación concedidas a un sistema de información y comunicaciones por la Autoridad de Acreditación de Seguridad (AAS) para tratar ICUE en su entorno operativo, tras la validación formal del plan de seguridad y su correcta aplicación.

b) «Proceso de acreditación»: medidas necesarias y tareas requeridas con anterioridad a la acreditación por la AAS. Estas medidas y tareas se especificarán en una norma del proceso de acreditación.

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

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

e) «Riesgo»: 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.

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

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

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

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

Artículo 36

SIC que manejen ICUE

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

2. Para los SIC que manejen ICUE, el cumplimiento de la política de seguridad de los sistemas de información de la Comisión, tal como se establece en la Decisión de la Comisión C(2006) 3602, implica que ([1]):

a) se aplicará el enfoque «planear-ejecutar-verificar-actuar» a la ejecución de la política de seguridad de los sistemas de información durante todo el ciclo de vida del sistema de información;

b) las necesidades en materia de seguridad deberán determinarse a partir de una evaluación del impacto en la actividad;

c) el sistema de información y los datos que contiene deberán someterse a una clasificación formal de los activos;

([1]) C(2006) 3602, de 16 de agosto de 2006, relativa a la seguridad de los sistemas de información utilizados por la Comisión Europea.

d) las medidas de protección obligatorias determinadas por la política de seguridad de los sistemas de información deberán ponerse en práctica;

e) deberá aplicarse un proceso de gestión de riesgos, que consta de las siguientes etapas: identificación de amenazas y vulnerabilidades, evaluación del riesgo, gestión del riesgo, aceptación del riesgo y comunicación del riesgo;

f) se definirá, aplicará, verificará y revisará un plan de seguridad que incluya la política de seguridad y los procedimientos operativos de seguridad.

3. Todo el personal involucrado en el diseño, desarrollo, prueba, operación, gestión o utilización de los SIC que manejen ICUE notificará a la AAS todos los posibles puntos débiles, incidentes, fallos de seguridad o comprometimientos que puedan tener un impacto en la protección del SIC o de la ICUE que contenga.

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

a) se dará preferencia a los productos que hayan sido aprobados por el Consejo o por el Secretario General del Consejo, en su calidad de autoridad de certificación criptológica del Consejo, por recomendación del grupo de expertos de seguridad de la Comisión;

b) cuando ello esté justificado por motivos operativos específicos, la Autoridad de Certificación Criptológica de la Comisión (ACC) podrá, por recomendación del grupo de expertos de seguridad de la Comisión, dispensar del cumplimiento de los requisitos a que se refiere la letra a) y otorgar una aprobación provisional durante un período específico.

5. Durante la transmisión, tratamiento y almacenamiento de la ICUE por medios electrónicos se emplearán productos criptográficos homologados. Sin perjuicio de este requisito, se podrán aplicar procedimientos específicos en circunstancias urgentes o en configuraciones técnicas específicas previa aprobación de la ACC.

6. 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.

7. La autoridad de seguridad de la Comisión asumirá las funciones siguientes:

— Autoridad de Garantía de la Información (AGI),

— Autoridad de Acreditación de Seguridad (AAS),

— Autoridad TEMPEST,

— Autoridad de Certificación Criptológica (ACC),

— Autoridad de Distribución Criptológica (ADC).

8. La autoridad de seguridad de la Comisión designará para cada sistema a la Autoridad Operacional de Garantía de la Información (AOGI).

9. Las responsabilidades de las funciones descritas en los apartados 7 y 8 se determinarán en las normas de desarrollo.

Artículo 37

Acreditación de los SIC que manejen ICUE

1. Todos los SIC que manejen ICUE serán objeto de un proceso de acreditación, basado en los principios de la GI, cuyo nivel de detalle debe ser acorde con el nivel de protección requerido.

2. El proceso de acreditación incluirá la validación formal por la AAS de la Comisión del plan de seguridad para el SIC de que se trate a fin de obtener garantías de que:

a) se ha llevado a cabo de forma apropiada el proceso de gestión de riesgos, según lo indicado en el artículo 36, apartado 2;

b) el propietario del sistema ha asumido conscientemente el riesgo residual, y

c) se ha alcanzado un nivel de protección suficiente del SIC y de la ICUE manejada en él, de conformidad con la presente Decisión.

3. La AAS de la Comisión expedirá una declaración de acreditación que determinará el nivel máximo de clasificación de la ICUE que pueda manejarse en el SIC, así como las condiciones correspondientes para la operación. Esto se entenderá sin perjuicio de las tareas encomendadas al Consejo de Acreditación de Seguridad definido en el artículo 11 del Reglamento (UE) nº 512/2014 del Parlamento Europeo y del Consejo ([1]).

4. Un Consejo de Acreditación de Seguridad conjunto se encargará de la acreditación de los SIC de la Comisión en los que participen varias partes. Estará integrado por un representante de la AAS de cada parte, y lo presidirá un representante de la AAS de la Comisión.

5. El proceso de acreditación constará de una serie de tareas que deberán asumir las partes interesadas. La responsabilidad de la preparación de los expedientes de acreditación y la documentación será plenamente del propietario del SIC.

6. La acreditación será competencia de la AAS de la Comisión, que, en cualquier momento en el ciclo de vida del SIC, tendrá derecho a:

a) exigir que se aplique un proceso de acreditación;

b) auditar o inspeccionar el SIC;

c) cuando dejen de cumplirse las condiciones de funcionamiento, exigir la definición y aplicación efectiva de un plan de mejora de la seguridad en un plazo bien definido, pudiendo retirar el permiso para operar el SIC hasta que se cumplan de nuevo las condiciones para la operación.

7. El proceso de acreditación se establecerá en una norma sobre el proceso de acreditación de los SIC que manejen ICUE, que deberá adoptarse de conformidad con el artículo 10, apartado 3, de la Decisión C(2006) 3602.

Artículo 38

Circunstancias de urgencia

1. No obstante lo dispuesto en el presente capítulo, podrán aplicarse los procedimientos específicos que se describen a continuación en casos de urgencia, por ejemplo, en situaciones de crisis, conflicto o guerra, inminentes o reales, o en circunstancias operativas excepcionales.

2. 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, y

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

3. En las circunstancias expuestas en el apartado 1, 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.

4. Se presentará posteriormente un informe a la autoridad competente y al grupo de expertos de seguridad de la Comisión.

CAPÍTULO 6

SEGURIDAD INDUSTRIAL

Artículo 39

Principios básicos

1. Por «seguridad industrial» se entenderá la aplicación de medidas encaminadas a garantizar la protección de la ICUE:

a) en el marco de los contratos clasificados, por:

   i) los candidatos o licitadores a lo largo de todo el procedimiento de licitación y contratación,

   ii) los contratistas o subcontratistas durante toda la vigencia de los contratos clasificados;

([1]) Reglamento (UE) nº 512/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por el que se modifica el Reglamento (UE) nº 912/2010, por el que se crea la Agencia del GNSS Europeo (DO L 150 de 20.5.2014, p. 72).

b) en el marco de los acuerdos de subvención clasificados, por:

i) los solicitantes durante los procedimientos de concesión de subvenciones;

ii) los beneficiarios a lo largo de todo el ciclo de vida de los acuerdos de subvención clasificados.

2. Dichos contratos o acuerdos de subvención no implicarán información clasificada TRES SECRET UE/EU TOP SECRET.

3. Salvo indicación en contrario, las disposiciones del presente capítulo relativas a contratos clasificados o contratistas serán también aplicables a los subcontratos clasificados o subcontratistas.

Artículo 40

Definiciones

A efectos del presente capítulo se entenderá por:

a) «Contrato clasificado»: contrato marco o contrato, conforme a lo dispuesto en el Reglamento (CE, Euratom) nº 1605/2002 de la Comisión ([1]), firmado por la Comisión o uno de sus servicios con un contratista para el suministro de bienes muebles o inmuebles, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.

b) «Subcontrato clasificado»: contrato celebrado por un contratista de la Comisión o alguno de sus servicios, con otro contratista (denominado «subcontratista») para el suministro de bienes muebles o inmuebles, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.

c) «Acuerdo de subvención clasificado»: acuerdo en virtud del cual la Comisión concede una subvención, tal como se indica en la parte I, título VI, del Reglamento (CE, Euratom) nº 1605/2002, cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.

d) «Autoridad de Seguridad Designada» (ASD): 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.

Artículo 41

Procedimiento para los contratos o acuerdos de subvención clasificados

1. Cada servicio de la Comisión, en calidad de órgano de contratación, velará por que las normas mínimas sobre seguridad industrial establecidas en el presente capítulo se mencionen o incorporen en el contrato, y se cumplan, a la hora de adjudicar contratos o acuerdos de subvención clasificados.

2. A efectos de lo dispuesto en el apartado 1, los servicios competentes de la Comisión solicitarán el dictamen de la Dirección General de Recursos Humanos y Seguridad, y, en particular, de su Dirección de Seguridad, y velarán por que los modelos de contratos y subcontratos y los modelos de acuerdos de subvención incluyan disposiciones que reflejen los principios básicos y las normas mínimas de protección de la ICUE que deben cumplir los contratistas y subcontratistas, y los beneficiarios de acuerdos de subvención, respectivamente.

3. La Comisión cooperará estrechamente con la ANS, la ASD o cualquier otra autoridad competente de los Estados miembros de que se trate.

4. Cuando un órgano de contratación se proponga poner en marcha un procedimiento destinado a celebrar un contrato o un acuerdo de subvención clasificado, solicitará el dictamen de la autoridad de seguridad de la Comisión sobre cuestiones relativas a la naturaleza y elementos clasificados del procedimiento, en todas sus fases.

5. En las normas de desarrollo sobre seguridad industrial, previa consulta al grupo de expertos de seguridad de la Comisión, se establecerán plantillas y modelos de contratos y subcontratos clasificados, acuerdos de subvención clasificados, anuncios de contrato, orientación sobre las circunstancias en que se requiere una habilitación de seguridad de establecimiento, instrucciones de seguridad de un programa o proyecto, cláusulas sobre aspectos de la seguridad, visitas, y transmisión y transporte de ICUE en virtud de contratos o acuerdos de subvención clasificados.

([1]) Reglamento (CE, Euratom) nº 1605/2002 del Consejo, de 25 de junio de 2002, por el que se aprueba el Reglamento financiero aplicable al presupuesto general de las Comunidades Europeas (DO L 248 de 16.9.2002, p. 1).

6. La Comisión podrá celebrar contratos o acuerdos de subvención clasificados que confíen tareas que conlleven el acceso a ICUE o su manejo o almacenamiento por operadores económicos registrados en un Estado miembro o en un tercer Estado con los que se haya celebrado un acuerdo o un convenio administrativo de conformidad con lo dispuesto en el capítulo 7 de la presente Decisión.

Artículo 42

Elementos de seguridad en un contrato o acuerdo de subvención clasificado

1. Los contratos o contratos de subvención clasificados incluirán los siguientes elementos de seguridad:

Instrucciones de seguridad de un programa o proyecto

a) Las «Instrucciones de seguridad de un programa o proyecto» son una lista de procedimientos de seguridad aplicables a un programa o proyecto específico para tipificar los procedimientos de seguridad. Pueden ser objeto de revisión a lo largo de la ejecución del programa o proyecto.

b) La Dirección General de Recursos Humanos y Seguridad elaborará Instrucciones de seguridad de un programa o proyecto genéricas. Los servicios de la Comisión responsables de los programas o proyectos que conlleven el manejo o almacenamiento de ICUE podrán desarrollar, cuando proceda, instrucciones específicas, que se basarán en dichas instrucciones genéricas.

c) Se desarrollarán Instrucciones de seguridad de un programa o proyecto, en particular, para programas y proyectos caracterizados por su gran alcance, importancia o complejidad, o por la multiplicidad o diversidad de los contratistas, beneficiarios y otros socios y partes interesadas, por ejemplo en lo que respecta a su situación jurídica. La Instrucciones de seguridad de un programa o proyecto serán elaboradas por el servicio o servicios de la Comisión que gestionen el programa o proyecto, en estrecha colaboración con la Dirección General de Recursos Humanos y Seguridad.

d) La Dirección General de Recursos Humanos y Seguridad someterá a la apreciación del grupo de expertos de seguridad de la Comisión tanto las Instrucciones de seguridad de un programa o proyecto genéricas como las específicas.

Cláusula sobre aspectos de la seguridad

a) «Cláusula sobre aspectos de la seguridad»: conjunto de condiciones contractuales especiales impuestas por el órgano de contratación 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.

b) 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 la seguridad y será parte integrante de un contrato o subcontrato o acuerdo de subvención clasificado.

c) 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 órgano de contratación se asegurará de que la cláusula indique que el incumplimiento de dichos estándares mínimos podrá ser motivo suficiente para la rescisión del contrato o del acuerdo de subvención.

2. Tanto las Instrucciones de seguridad de un programa o proyecto como las cláusulas sobre aspectos de la seguridad incluirán como elemento de seguridad obligatorio una guía de clasificación de seguridad:

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

b) Antes de convocar una licitación o adjudicar un contrato clasificado, el servicio de la Comisión, como órgano de contratación, determinará la clasificación de seguridad de toda información que deba proporcionarse a los candidatos y licitadores o contratistas, así como la clasificación de seguridad de toda información que haya de producir el contratista. Para ello, elaborará una guía de clasificación de la seguridad, que deberá emplearse en la ejecución del contrato, con arreglo a lo dispuesto en la presente Decisión y sus normas de desarrollo, previa consulta a la autoridad de seguridad de la Comisión.

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

i) al elaborar una guía de clasificación de seguridad, el servicio de la Comisión, como órgano de contratación, 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;

ii) el grado general de clasificación del contrato no podrá ser inferior al mayor grado de clasificación de cualquiera de sus elementos; y

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

Artículo 43

Acceso a la ICUE del personal de los beneficiarios y los contratistas

El órgano de contratación o la autoridad que concede la subvención se asegurará de que el contrato o acuerdo de subvención clasificado incluya disposiciones que indiquen que al personal del contratista, subcontratista o beneficiario que, para la ejecución del contrato, subcontrato o acuerdo de subvención clasificado, precise el acceso a ICUE, solo se le concederá dicho acceso si:

a) la persona posee una autorización de seguridad para el nivel adecuado u otra autorización debidamente emitida para la que se haya comprobado su necesidad de conocer la información;

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

c) ha sido habilitada para el nivel correspondiente para la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET por la ANS, la ASD o cualquier otra autoridad competente.

Artículo 44

Habilitación de seguridad de establecimiento

1. «Habilitación de seguridad de establecimiento»: certificación administrativa por parte de una ANS o ASD o cualquier otra autoridad de seguridad competente 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.

2. La habilitación de seguridad de establecimiento concedida por la ANS, 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 un operador económico puede proteger la ICUE del nivel de clasificación que corresponda (CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET) en sus instalaciones, deberá presentarse a la autoridad de seguridad de la Comisión, que la remitirá al servicio de la Comisión que actúe como órgano de contratación o autoridad que concede la subvención, antes de que pueda facilitarse acceso a la ICUE a un candidato, licitador o contratista, o solicitante o beneficiario de la subvención.

3. En su caso, el órgano de contratación notificará, a través de la autoridad de seguridad de la Comisión, la ANS adecuada, la ASD o cualquier otra autoridad de seguridad competente, que es necesario contar con una habilitación de seguridad de establecimiento para la ejecución del contrato. Se exigirá una habilitación de seguridad de establecimiento o una HPS en los casos en que, en el transcurso del procedimiento de adjudicación de contratos o de concesión de subvenciones, deba facilitarse ICUE clasificada en el nivel CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

4. El órgano de contratación o la autoridad que conceda la subvención no adjudicará un contrato o un acuerdo de subvención clasificado al licitador seleccionado antes de haber recibido de la ANS, 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.

5. La ANS, la ASD o cualquier otra autoridad de seguridad competente que haya expedido una habilitación de seguridad de establecimiento notificará a la autoridad de seguridad de la Comisión los cambios que afecten a dicha habilitación. Esta autoridad, a su vez, informará de ello al servicio de la Comisión que actúe como órgano de contratación o autoridad que concede la subvención. En el caso de los subcontratos, se informará al respecto a la ANS, la ASD o cualquier otra autoridad de seguridad competente.

6. 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 el órgano de contratación o la autoridad que concede la subvención rescinda un contrato clasificado o excluya a un licitador de la licitación. Se incluirá una disposición a tal efecto en el modelo de contratos y acuerdos de subvención que se desarrollen.

Artículo 45

Disposiciones para contratos y acuerdos de subvención clasificados

1. Cuando se facilite ICUE a un candidato, licitador o solicitante durante el procedimiento de licitación, la convocatoria de licitación o convocatoria de propuestas deberá contener una cláusula que obligue a los candidatos, licitadores o solicitantes que no presenten una oferta o propuesta o que no resulten seleccionados a devolver toda la documentación clasificada en un plazo determinado.

2. El órgano de contratación o la autoridad que concede la subvención notificará, a través de la autoridad de seguridad de la Comisión, a la ANS competente, la ASD o cualquier otra autoridad de seguridad competente, el hecho de que se ha adjudicado un contrato o un acuerdo de subvención, y los datos pertinentes, tales como el nombre del contratista o contratistas o los beneficiarios, la duración del contrato y el nivel máximo de clasificación.

3. Cuando tales contratos o acuerdos de subvención finalicen, el órgano de contratación o la autoridad que concede la subvención lo notificará sin demora, a través de la autoridad de seguridad de la Comisión, a la ANS, la ASD o cualquier otra autoridad de seguridad competente del Estado miembro en que esté registrado el contratista o el beneficiario de la subvención.

4. Por regla general, el contratista o el beneficiario de la subvención estará obligado a devolver al órgano de contratación o la autoridad que concede la subvención, al término del contrato clasificado o del acuerdo de subvención, o de la participación de un beneficiario de la subvención, toda la ICUE que obre en su posesión.

5. En la cláusula sobre aspectos de la seguridad se incluirán disposiciones específicas para la eliminación de ICUE durante la ejecución del contrato clasificado o el acuerdo de subvención clasificado.

6. En caso de que el contratista o el beneficiario de la subvención esté autorizado para conservar ICUE al término de un contrato o acuerdo de subvención clasificado, las normas mínimas contenidas en la presente Decisión seguirán siendo de obligado cumplimiento y la confidencialidad de la ICUE será protegida por el titular del contrato o el beneficiario de la subvención.

Artículo 46

Disposiciones específicas para los contratos clasificados

1. Las condiciones pertinentes para la protección de la ICUE en que un contratista podrá subcontratar se definirán en el pliego de condiciones y en el contrato.

2. Antes de subcontratar cualquier parte de un contrato clasificado, el contratista deberá obtener el permiso correspondiente del órgano de contratación. No podrá adjudicarse un subcontrato que implique el acceso a ICUE a subcontratistas registrados en un tercer país, salvo si existe un marco reglamentario para la seguridad de la información con arreglo a lo dispuesto en el capítulo 7.

3. 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 del órgano de contratación.

4. Respecto de la ICUE producida o manejada por el contratista, la Comisión será considerada el originador, y los derechos que asistan al originador serán ejercidos por el órgano de contratación.

Artículo 47

Visitas en relación con contratos clasificados

1. Cuando el personal de la Comisión, de los contratistas o de los beneficiarios de subvenciones 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 o un acuerdo de subvención clasificado, se organizarán visitas, en contacto con las ANS, las ASD o cualquier otra autoridad de seguridad competente. La autoridad de seguridad de la Comisión será informada de dichas visitas. Sin embargo, en el contexto de programas o proyectos específicos, las ANS, las ASD o cualquier otra autoridad de seguridad competente también podrán acordar un procedimiento que permita organizar directamente dichas visitas.

2. Todos los visitantes deberán estar en posesión de una habilitación de seguridad adecuada y tener necesidad de conocer para poder acceder a la ICUE relacionada con el contrato clasificado.

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

4. En las normas de desarrollo se establecerán disposiciones más detalladas.

5. Será obligatorio el cumplimiento de las disposiciones en materia de visitas en relación con los contratos clasificados establecidas en la presente Decisión y en las normas de desarrollo a que se refiere el apartado 4.

Artículo 48

Transmisión y transporte de ICUE en relación con contratos clasificados o acuerdos de subvención clasificados

1. Por lo que se refiere a la transmisión de ICUE por medios electrónicos, se aplicarán las disposiciones pertinentes del capítulo 5 de la presente Decisión.

2. Por lo que se refiere al transporte de ICUE, se aplicarán las disposiciones pertinentes del capítulo 4 de la presente Decisión y sus normas de desarrollo, de conformidad con las disposiciones legales y reglamentarias nacionales.

3. 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) 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;

d) en la medida de lo posible, los viajes evitarán las paradas intermedias y se completarán con toda la rapidez que las circunstancias permitan;

e) 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.

Artículo 49

Transmisión de ICUE a contratistas o beneficiarios de subvenciones establecidos en terceros Estados

La ICUE se transmitirá a los beneficiarios de subvenciones o contratistas establecidos en terceros Estados de conformidad con las medidas de seguridad acordadas entre la autoridad de seguridad de la Comisión, el servicio de la Comisión como órgano de contratación o autoridad que concede la subvención, y la ANS, la ASD o cualquier otra autoridad de seguridad competente del Estado tercero en el que esté registrado el contratista o el beneficiario de la subvención.

Artículo 50

Manejo de información clasificada con grado RESTREINT UE/EU RESTRICTED en el contexto de los contratos clasificados o los acuerdos de subvención clasificados

1. La protección de información clasificada de grado RESTREINT UE/EU RESTRICTED manejada o almacenada en virtud de contratos o acuerdos de subvención clasificados se basará en los principios de proporcionalidad y de relación coste-eficacia.

2. No se exigirá la habilitación de seguridad de establecimiento ni una HPS en el contexto de los contratos clasificados o los acuerdos de subvención clasificados que impliquen el manejo de información clasificada en el nivel RESTREINT UE/EU RESTRICTED.

3. Cuando un contrato o acuerdo de subvención implique el manejo de información clasificada de grado RESTREINT UE/EU RESTRICTED en un SIC gestionado por un contratista o beneficiario de una subvención, el órgano de contratación o la autoridad que concede la subvención deberá garantizar, previa consulta a la autoridad de seguridad de la Comisión, que el contrato o el acuerdo de subvención especifique los requisitos técnicos y administrativos necesarios relativos a la acreditación o aprobación del SIC en proporción al riesgo evaluado, teniendo en cuenta todos los factores pertinentes. El ámbito de la acreditación o aprobación de dicho SIC se determinará mediante acuerdo entre la autoridad de seguridad de la Comisión y la ANS o ASD correspondiente.

CAPÍTULO 7

INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON OTRAS INSTITUCIONES, ÓRGANOS, ORGANISMOS Y OFICINAS DE LA UNIÓN, CON LOS ESTADOS MIEMBROS Y CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

Artículo 51

Principios básicos

1. En caso de que la Comisión o uno de sus servicios determine que existe la necesidad de intercambiar ICUE con otra institución, órgano, organismo u oficina de la Unión, o con un tercer Estado o una organización internacional, se tomarán las medidas necesarias para establecer un marco jurídico o administrativo adecuado a tal efecto, que podrá incluir acuerdos sobre seguridad de la información o acuerdos administrativos celebrados de conformidad con la normativa pertinente.

2. Sin perjuicio de lo dispuesto en el artículo 57, solo se podrá intercambiar ICUE con otra institución, órgano, organismo u oficina de la Unión, o con un tercer Estado o una organización internacional, siempre que esté vigente tal marco jurídico o administrativo adecuado, y que existan suficientes garantías de que la institución, órgano, organismo u oficina de la Unión, o el tercer Estado u organización internacional de que se trate aplica principios básicos y normas mínimas equivalentes para la protección de la información clasificada.

Artículo 52

Intercambio de ICUE con otras instituciones, órganos, organismos y oficinas de la Unión

1. Antes de celebrar un acuerdo administrativo para el intercambio de ICUE con otra institución, órgano, organismo u oficina de la Unión, la Comisión recabará garantías de que la institución, órgano u organismo de que se trate:

a) dispone de un marco reglamentario para la protección de la ICUE que establezca principios básicos y normas mínimas equivalentes a las previstas en la presente Decisión y sus normas de desarrollo;

b) aplica normas de seguridad y directrices en lo que respecta a la seguridad del personal, la seguridad física, la gestión de la seguridad de la ICUE y la seguridad de los sistemas de información y comunicaciones (SIC), que garanticen un nivel de protección de la ICUE equivalente al que se concede en la Comisión;

c) señale como ICUE la información clasificada que cree.

2. La Dirección General de Recursos Humanos y Seguridad, en estrecha cooperación con otros servicios competentes de la Comisión, será el servicio responsable de la Comisión para la celebración de acuerdos administrativos para el intercambio de ICUE con otras instituciones, órganos, organismos y agencias de la Unión.

3. Por regla general, los acuerdos administrativos adoptarán la forma de un canje de notas, firmado por el director general de Recursos Humanos y Seguridad en nombre de la Comisión.

4. Antes de celebrar un acuerdo administrativo de intercambio de ICUE, la autoridad de seguridad de la Comisión realizará una visita de evaluación destinada a evaluar el marco regulador para la protección de la ICUE y determinar la eficacia de las medidas establecidas para la protección de la ICUE. El acuerdo administrativo entrará en vigor, y se intercambiará ICUE, únicamente si los resultados de esta visita de evaluación son satisfactorios y se cumplen las recomendaciones formuladas a raíz de la visita. Se realizarán visitas de evaluación de seguimiento periódicas para comprobar que el acuerdo administrativo se cumple y que las medidas de seguridad establecidas siguen respetando los principios básicos y las normas mínimas acordadas.

5. Dentro de la Comisión, el registro de ICUE gestionado por la Secretaría General será, por regla general, el punto principal de entrada y salida para los intercambios de información clasificada con otras instituciones, órganos, organismos u oficinas de la Unión. No obstante, en caso de que, por razones de seguridad, de organización o de funcionamiento sea más adecuado para la protección de la ICUE, los registros locales de ICUE establecidos en los servicios de la Comisión de conformidad con la presente Decisión y sus normas de desarrollo funcionarán como punto de entrada y salida de la información clasificada con respecto a los asuntos que sean competencia de los servicios de la Comisión interesados.

6. El grupo de expertos de la Comisión en materia de seguridad será informado del proceso de celebración de acuerdos administrativos con arreglo a lo dispuesto en el apartado 2.

Artículo 53

Intercambio de ICUE con los Estados miembros

1. La ICUE podrá intercambiarse y cederse a los Estados miembros siempre que estos protejan dicha información con arreglo a los requisitos aplicables a la información clasificada que lleve una clasificación de seguridad nacional del nivel de clasificación equivalente según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el anexo I.

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

Artículo 54

Intercambio de ICUE con terceros Estados y organizaciones internacionales

1. Cuando la Comisión determine que tiene la necesidad a largo plazo de intercambiar información clasificada con terceros Estados u organizaciones internacionales, se tomarán las medidas necesarias para establecer un marco jurídico o administrativo adecuado a tal efecto, que podrá incluir acuerdos sobre seguridad de la información o acuerdos administrativos celebrados de conformidad con la normativa pertinente.

2. Los acuerdos de seguridad de la información o los acuerdos administrativos a que se refiere el apartado 1 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 sean equivalentes a las que establece la presente Decisión.

3. La Comisión podrá celebrar acuerdos administrativos de conformidad con lo dispuesto en el artículo 56 cuando el nivel de clasificación de la ICUE no sea en general superior a RESTREINT UE/EU RESTRICTED.

4. Los acuerdos administrativos para el intercambio de información clasificada a que se refiere el apartado 3 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. El grupo de expertos de seguridad de la Comisión deberá ser consultado sobre la celebración de los acuerdos de seguridad de la información o acuerdos administrativos.

5. La decisión de ceder ICUE originada en la Comisión a un tercer Estado u organización internacional será adoptada por el servicio de la Comisión, como originador de la ICUE dentro de la Comisión, caso por caso, en función de la naturaleza y del contenido de dicha 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, o del material fuente que contenga, no sea la Comisión, el servicio de la Comisión que posea esa información clasificada deberá recabar el consentimiento escrito del originador antes de comunicarla. En caso de que no sea posible determinar el originador, el servicio de la Comisión que tenga en su poder esa información clasificada asumirá la responsabilidad de aquel tras consultar al grupo de expertos de seguridad de la Comisión.

Artículo 55

Acuerdos de seguridad de la información

1. Los acuerdos de seguridad de la información con terceros Estados u organizaciones internacionales se celebrarán de conformidad con el artículo 218 del TFUE.

2. Los acuerdos de seguridad de la información:

a) establecerán los principios básicos y las normas mínimas aplicables al intercambio de información clasificada entre la Unión y un tercer Estado u organización internacional;

b) 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;

c) establecerán que, antes de intercambiarse la información clasificada en virtud del acuerdo, se comprobará que la parte receptora es capaz de proteger y salvaguardar la información clasificada que se le haya facilitado, de manera adecuada.

3. La Comisión consultará, cuando se determine una necesidad de intercambiar información clasificada de conformidad con el artículo 51, apartado 1, al Servicio Europeo de Acción Exterior, a la Secretaría General del Consejo y a otras instituciones y órganos de la Unión, según proceda, a fin de establecer si debe presentarse una recomendación de conformidad con el artículo 218, apartado 3, del TFUE.

4. No se intercambiará ICUE por medios electrónicos a menos que se haya previsto explícitamente en el acuerdo de seguridad de la información o en las disposiciones técnicas de aplicación.

5. Dentro de la Comisión, el registro de ICUE gestionado por la Secretaría General será, por regla general, el punto principal de entrada y salida para los intercambios de información clasificada con terceros Estados y organizaciones internacionales. No obstante, en caso de que, por razones de seguridad, de organización o de funcionamiento sea más adecuado para la protección de la ICUE, los registros locales de información clasificada establecidos en los servicios de la Comisión de conformidad con lo dispuesto en la presente Decisión y sus normas de desarrollo, funcionarán como punto de entrada y salida de la información clasificada con respecto a los asuntos que sean competencia de los servicios de la Comisión interesados.

6. Con el fin de evaluar la eficacia de las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional de que se trate, la Comisión, en colaboración con otras instituciones, órganos u organismos de la Unión, participará en visitas de evaluación de mutuo acuerdo con el tercer Estado o la organización internacional de que se trate. En dichas visitas se evaluará:

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.

Artículo 56

Disposiciones administrativas

1. En los casos en que exista la necesidad a largo plazo, en el contexto de un marco político o jurídico de la Unión, de intercambiar información clasificada, en principio no superior al grado RESTREINT UE/EU RESTRICTED, con un tercer Estado o una organización internacional, y cuando la autoridad de seguridad de la Comisión, previa consulta al grupo de expertos de seguridad de la Comisión, haya establecido, en particular, que la parte en cuestión no cuenta con un sistema de seguridad suficientemente desarrollado como para que se pueda celebrar un acuerdo de seguridad de la información, la Comisión podría decidir celebrar un acuerdo administrativo con las autoridades competentes del tercer Estado o la organización internacional de que se trate.

2. Por regla general, tales acuerdos administrativos adoptarán la forma de un canje de notas.

3. Se realizará una visita de evaluación antes de la celebración del acuerdo. El grupo de expertos de seguridad de la Comisión será informado del resultado de la visita de evaluación. Cuando existan razones excepcionales para el intercambio urgente de información clasificada, podrá cederse la ICUE siempre que se haga todo lo posible para realizar una visita de evaluación cuanto antes.

4. No se intercambiará ICUE por medios electrónicos a menos que se haya establecido explícitamente en el acuerdo administrativo.

Artículo 57

Cesión *ad hoc* con carácter excepcional de ICUE

1. En caso de que no exista un acuerdo de seguridad de la información o un acuerdo administrativo en vigor, y cuando la Comisión o uno de sus servicios determine que es necesario, a título excepcional, en el contexto de un marco jurídico o político de la Unión, ceder ICUE a un tercer Estado o a una organización internacional, la autoridad de seguridad de la Comisión 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.

2. La decisión de ceder ICUE al tercer Estado u organización internacional de que se trate, previa consulta al grupo de expertos de seguridad de la Comisión, la tomará la Comisión sobre la base de una propuesta presentada por el miembro de la Comisión responsable de los asuntos de seguridad.

3. Una vez que haya tomado la Comisión la decisión de ceder ICUE, y con el consentimiento previo por escrito del originador, incluidos los originadores del material fuente que contenga, el servicio competente de la Comisión 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.

CAPÍTULO 8

DISPOSICIONES FINALES

Artículo 58

Sustitución de anteriores decisiones

La presente Decisión deroga y sustituye la Decisión 2001/844/CE, CECA, Euratom de la Comisión ([1]).

Artículo 59

Información clasificada producida antes de la entrada en vigor de la presente Decisión

1. Toda la ICUE clasificada conforme a la Decisión 2001/844/CE, CECA, Euratom, seguirá estando protegida de acuerdo con las disposiciones pertinentes de la presente Decisión.

2. Toda la información clasificada en posesión de la Comisión en la fecha de entrada en vigor la Decisión 2001/844/CE, CECA, Euratom, con excepción de la información clasificada de Euratom:

a) en caso de proceder de la Comisión, se considerará que se ha reclasificado como «RESTREINT UE» por defecto, a no ser que su autor hubiese decidido darle otra clasificación antes del 31 de enero de 2002 y hubiese informado a todos los destinatarios del documento de que se trate;

b) en caso de que el autor sea ajeno a la Comisión, conservará su clasificación original y será tratada por consiguiente como ICUE de nivel equivalente, a no ser que el autor dé su consentimiento a la desclasificación o reducción del grado de clasificación de la información.

Artículo 60

Normas de desarrollo y consignas de seguridad

1. En caso necesario, la adopción de las normas de desarrollo de la presente Decisión será objeto de una nueva decisión de habilitación de la Comisión en favor del miembro de la Comisión responsable de las cuestiones de seguridad, de plena conformidad con el Reglamento interno.

2. Después de haber sido facultada a raíz de la Decisión de la Comisión anteriormente mencionada, el miembro de la Comisión responsable de las cuestiones de seguridad podrá elaborar consignas de seguridad que se establezcan directrices de seguridad y las mejores prácticas en el ámbito de aplicación de la presente Decisión y de las normas de desarrollo.

3. La Comisión podrá delegar las tareas mencionadas en los apartados 1 y 2 del presente artículo en el director general de la Dirección General de Recursos Humanos y Seguridad mediante una nueva decisión de delegación, de conformidad con el Reglamento interno.

Artículo 61

Entrada en vigor

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

Hecho en Bruselas, el 13 de marzo de 2015.

Por la Comisión

El Presidente

Jean-Claude JUNCKER

([1]) Decisión 2001/844/CE, CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno (DO L 317 de 3.12.2001, p. 1).

ANEXO I

EQUIVALENCIA DE LAS CLASIFICACIONES DE SEGURIDAD

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Bélgica	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	véase la nota (1)
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	véase la nota (3)
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
Luxemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungría	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
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

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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 ([4])	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	No hay equivalente ([5])	UK OFFICIAL-SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding no es una clasificación de seguridad en Bélgica. Bélgica maneja y protege la información «RESTREINT UE/EU RESTRICTED» de forma no menos rigurosa que las normas 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» de forma no menos rigurosa que las normas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

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

([5]) El Reino Unido maneja y protege la ICUE señalada como CONFIDENTIEL UE/EU CONFIDENTIAL con arreglo a los requisitos de protección de seguridad correspondientes a «UK SECRET».

ANEXO II

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 manejan ICUE
TI	Tecnologías de la información
TFUE	Tratado de Funcionamiento de la Unión Europea

ANEXO III

LISTA DE AUTORIDADES NACIONALES DE SEGURIDAD

BÉLGICA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. Secretariat: +32 25014542
Fax +32 25014596
Correo electrónico: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Fax +359 29873750
Correo electrónico: dksi@government.bg
Website: 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
Website: 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

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

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax +372 7170213
Correo electrónico: nsa@mod.gov.ee

GRECIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
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)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — 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

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
Website: www.uvns.hr

IRLANDA

National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

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

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

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

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

LUXEMBURGO

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

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
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax +356 25695321

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

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 22 58 57 944
fax +48 22 58 57 443
Correo electrónico: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

RUMANÍA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Fax +40 212240714
Correo electrónico: nsa.romania@nsa.ro
Website: www.orniss.ro

ESLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
Correo electrónico: gp.uvtp@gov.si

ESLOVAQUIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Website: www.nbusr.sk

FINLANDIA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax +358 916055140
Correo electrónico: NSA@formin.fi

SUECIA

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Fax +46 87231176
Correo electrónico: ud-nsa@foreign.ministry.se

REINO UNIDO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
Correo electrónico: UK-NSA@cabinet-office.x.gsi.gov.uk