II

(Actos cuya publicación no es una condición para su aplicabilidad)

COMISIÓN

DECISIÓN DE LA COMISIÓN
de 29 de noviembre de 2001
por la que se modifica su Reglamento interno

[notificada con el número C(2001) 3031]

(2001/844/CE, CECA, Euratom)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 218,

Visto el Tratado constitutivo de la Comunidad Europea del Carbón y del Acero, y, en particular, su artículo 16,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica y, en particular, su artículo 131,

Visto el Tratado de la Unión Europea, y, en particular, el apartado 1 de su artículo 28 y el apartado 1 de su artículo 41.

DECIDE:

Artículo 1

Las disposiciones de la Comisión en materia de seguridad, cuyo texto figura en el anexo de la presente Decisión, se añaden al Reglamento interno de la Comisión como anexo.

Artículo 2

La presente Decisión entrará en vigor el día de su publicación en el *Diario Oficial de las Comunidades Europeas*.

Será aplicable a partir del 1 de diciembre de 2001.

Hecho en Bruselas, el 29 de noviembre de 2001.

Por la Comisión
El Presidente
Romano PRODI

ANEXO

DISPOSICIONES DE LA COMISIÓN EN MATERIA DE SEGURIDAD

Considerando lo siguiente:

(1) A fin de desarrollar las actividades de la Comisión en los ámbitos que exigen un determinado grado de confidencialidad, es conveniente establecer un sistema exhaustivo de seguridad aplicable a la Comisión, las demás instituciones, órganos, oficinas y agencias establecidos en virtud del Tratado CE o del Tratado de la Unión Europea o sobre la base de dichos Tratados, y los Estados miembros, así como cualquier otro destinatario de información clasificada de la Unión Europea, denominada en lo sucesivo «información clasificada de la UE».

(2) A fin de salvaguardar la eficacia del sistema de seguridad así establecido, la Comisión sólo facilitará información clasificada de la UE a los órganos externos que ofrezcan garantías de que han adoptado todas las medidas necesarias para aplicar normas estrictamente equivalentes a las presentes disposiciones.

(3) Las presentes disposiciones se adoptan sin perjuicio de lo dispuesto en el Reglamento 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 [1], el Reglamento (CE) nº 1588/90 del Consejo, de 11 de junio de 1990, relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico [2], y la Decisión C(95) 1510 final de la Comisión, de 23 de noviembre de 1995, sobre la protección de los sistemas informáticos.

(4) El sistema de seguridad de la Comisión se basa en los principios presentados en la Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo [3], a fin de garantizar el correcto funcionamiento del proceso de adopción de decisiones de la Unión.

(5) La Comisión subraya la importancia de que, cuando resulte adecuado, las demás instituciones queden asociadas a las normas de confidencialidad necesarias para proteger los intereses de la Unión y de sus Estados miembros.

(6) La Comisión reconoce la necesidad de crear su propio concepto de seguridad, teniendo en cuenta todos los elementos relativos a la seguridad y el carácter específico de la Comisión como institución.

(7) Las presentes disposiciones se adoptan sin perjuicio de lo dispuesto en el artículo 255 del Tratado y el 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 [4].

Artículo 1

Se establecen en el anexo las normas de la Comisión en materia de seguridad.

Artículo 2

1. El miembro de la Comisión encargado de los asuntos de seguridad adoptará las medidas adecuadas para garantizar que, al tratarse información clasificada de la UE, se cumplan en la Comisión las normas a que se refiere el artículo 1 por parte de los funcionarios y otros agentes de la Comisión, del personal enviado a la Comisión en comisión de servicio, y en todos los locales de la Comisión, incluidas sus Representaciones y Oficinas en la Unión y sus Delegaciones en terceros países, así como por parte de los contratistas externos a la Comisión.

2. Los Estados miembros, las demás instituciones, órganos, oficinas y agencias establecidos en virtud o sobre la base de los Tratados estarán autorizados para recibir información clasificada de la UE siempre y cuando garanticen que, cuando se trate este tipo de información, se cumplan en sus servicios y locales normas estrictamente equivalentes a las normas a que se refiere el artículo 1, en particular por parte de:

a) los miembros de las Representaciones Permanentes de los Estados miembros ante la Unión Europea, así como los miembros de las Delegaciones nacionales que asistan a reuniones de la Comisión o de sus órganos, o que participen en otras actividades de la Comisión;

b) otros miembros de las administraciones nacionales de los Estados miembros que traten información clasificada de la UE, con independencia de que ejerzan sus funciones en el territorio de los Estados miembros o en el extranjero;

c) los contratistas externos y el personal enviado en comisión de servicio que traten información clasificada de la UE.

[1] DO nº 17 de 6.10.1958, p. 406/58.
[2] DO L 151 de 15.6.1990, p. 1.
[3] DO L 101 de 11.4.2001, p. 1.
[4] DO L 145 de 31.5.2001, p. 43.

Artículo 3

Los países terceros, las organizaciones internacionales y demás órganos estarán autorizados para recibir información clasificada de la UE siempre y cuando garanticen que, cuando se trate este tipo de información, se cumplan normas estrictamente equivalentes a las normas a que se refiere el artículo 1.

Artículo 4

De conformidad con los principios básicos y las normas mínimas de seguridad recogidos en la Parte I del anexo, el miembro de la Comisión encargado de los asuntos de seguridad podrá adoptar medidas con arreglo a lo dispuesto en la Parte II del anexo.

Artículo 5

Las presentes disposiciones sustituirán, a partir de la fecha de su aplicación, a las siguientes:

a) Decisión C(94) 3282 de la Comisión, de 30 de noviembre de 1994, relativa a las medidas de seguridad aplicables a la información clasificada facilitada o transmitida en relación con las actividades de la Unión Europea;

b) Decisión C(1999) 423 de la Comisión, de 25 de febrero de 1999, relativa a los procedimientos por los que los funcionarios y demás empleados de la Comisión Europea pueden ser autorizados a tener acceso a la información clasificada en poder de la Comisión.

Artículo 6

A partir de la fecha de aplicación de las presentes disposiciones, toda la información clasificada en poder de la Comisión hasta esa fecha, a excepción de la información clasificada de Euratom:

a) en caso de proceder de la Comisión, se considerará como información que deba reclasificarse como «EU RESTRICTED» por defecto, a no ser que su autor decida darle otra clasificación antes del 31 de enero de 2002, en cuyo caso dicho autor informará 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 información clasificada de la UE de nivel equivalente, a no ser que el autor dé su consentimiento a la desclasificación o recalificación de la información.

ANEXO

NORMAS EN MATERIA DE SEGURIDAD

Índice

-

PARTE I: PRINCIPIOS BÁSICOS Y NORMAS MÍNIMAS DE SEGURIDAD

1. INTRODUCCIÓN

Las presentes disposiciones establecen los principios básicos y las normas mínimas de seguridad que deberán respetar de manera adecuada la Comisión, en todos sus lugares de trabajo, y todos los destinatarios de información clasificada de la UE, a fin de salvaguardar la seguridad y garantizar a cada uno el establecimiento de una norma común de protección.

2. PRINCIPIOS GENERALES

La política de seguridad de la Comisión forma parte integrante de su política general de gestión interna y está basada por lo tanto en los principios que regulan su política general.

Se trata de los principios de legalidad, transparencia, responsabilidad y subsidiariedad (proporcionalidad).

La legalidad indica la necesidad de permanecer estrictamente en el marco jurídico a la hora de ejecutar las funciones de seguridad y la necesidad de ajustarse a los requisitos jurídicos. Significa también que las responsabilidades en materia de seguridad deben basarse en las disposiciones legales adecuadas. Son plenamente aplicables las disposiciones del Estatuto y, especialmente, su artículo 17 relativo a la obligación del personal de observar discreción en relación con la información de la Comisión y su Título VI sobre el régimen disciplinario. Significa por último que las infracciones a la seguridad que son responsabilidad de la Comisión deben tratarse de forma coherente con la política de la Comisión sobre medidas disciplinarias y su política de cooperación con los Estados miembros en materia de justicia penal.

La transparencia indica la necesidad de claridad por lo que respecta a todas las normas y disposiciones relativas a la seguridad, de cierto equilibrio entre los distintos servicios y los diferentes sectores (seguridad física frente a protección de la información, etc.) y de una política coherente y estructurada de sensibilización a la seguridad. También establece la necesidad de unas directrices claras por escrito, relativas a la aplicación de las medidas de seguridad.

La responsabilidad significa que se definirán claramente las responsabilidades en el ámbito de la seguridad. Indica además la necesidad de proceder a pruebas periódicas a fin de comprobar si se asumen correctamente dichas responsabilidades.

La subsidiariedad, o proporcionalidad, significa que la seguridad se organizará al nivel más bajo posible y más próximo posible de las Direcciones Generales y los servicios de la Comisión. También indica que las actividades relacionadas con la seguridad se limitarán exclusivamente a aquellos elementos que la necesiten realmente. Significa por último que las medidas de seguridad serán proporcionales a los intereses que sea preciso proteger y a los riesgos reales o potenciales en torno a esos intereses, permitiendo una defensa que cause el mínimo trastorno posible.

3. FUNDAMENTOS DE LA SEGURIDAD

Los fundamentos de una seguridad óptima serán los siguientes:

a) en cada Estado miembro, una organización de seguridad nacional responsable de:

   1) recopilar y registrar la información confidencial en materia de espionaje, sabotaje, terrorismo y otras actividades subversivas y

   2) facilitar información y prestar asesoramiento a su Gobierno correspondiente y, a través de éste, a la Comisión, sobre la índole de las amenazas contra la seguridad y sobre los medios de protección frente a dichas amenazas;

b) en cada Estado miembro, y en la Comisión, una autoridad técnica en materia de seguridad de la información (INFOSEC), responsable de colaborar con la autoridad de seguridad correspondiente a fin de facilitar información y prestar asesoramiento sobre las amenazas técnicas contra la seguridad y los medios de protección frente a dichas amenazas;

c) una colaboración periódica entre los Ministerios y los servicios adecuados de las instituciones europeas con el fin de determinar y recomendar, según resulte apropiado:

   1) qué personas, información y recursos necesitan protección, y

   2) unas normas comunes de protección;

d) una estrecha colaboración entre la Oficina de Seguridad de la Comisión y los servicios de seguridad de las demás instituciones europeas, así como la Oficina de Seguridad de la OTAN.

4. PRINCIPIOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN

4.1. **Objetivos**

La seguridad de la información tendrá los siguientes objetivos principales:

a) proteger la información clasificada de la UE frente al espionaje, las situaciones de peligro o la divulgación no autorizada;

b) proteger la información de la UE tratada en los sistemas y redes de comunicación e información frente a las amenazas contra su confidencialidad, integridad y disponibilidad;

c) proteger los locales de la Comisión en los que se encuentra información de la UE frente al sabotaje y los daños intencionados;

d) en caso de fallo, evaluar el perjuicio causado, limitar sus consecuencias y adoptar las medidas necesarias para remediarlo.

4.2. **Definiciones**

En las presentes normas se entenderá por:

a) «información clasificada de la UE», toda información y material cuya divulgación no autorizada pueda causar perjuicio en distintos grados a los intereses de la UE, o de uno o varios Estados miembros, ya se origine dicha información en la UE o proceda de los Estados miembros, terceros países u organizaciones internacionales;

b) «documento», todo escrito, nota, acta, informe, memorándum, señal o mensaje, dibujo, fotografía, diapositiva, película, mapa, gráfico, plano, cuaderno, plantilla, papel carbón, máquina de escribir o cinta mecanográfica, cinta magnetofónica, casete, disco de ordenador, CD-ROM u otro medio físico en que se haya registrado información;

c) «material», todo documento según se define en la letra b), así como todo artículo de equipo, producido o en proceso de producción;

d) «necesidad de conocer», la necesidad de un empleado de tener acceso a información clasificada de la UE para poder desempeñar una función o tarea;

e) «autorización», la decisión del Presidente de la Comisión de permitir a una persona el acceso a información clasificada de la UE hasta un nivel determinado, sobre la base del resultado positivo de una comprobación de seguridad (investigación), llevada a cabo por una autoridad nacional de seguridad de acuerdo con la legislación nacional;

f) «clasificación», la asignación de un nivel adecuado de seguridad a la información cuya divulgación no autorizada podría causar perjuicio en distintos grados a los intereses de la Comisión o de los Estados miembros;

g) «recalificación» (downgrading — déclassement), la disminución del nivel de clasificación;

h) «desclasificación» (declassification — déclassification), la supresión de toda mención de clasificación;

i) «autor», la persona debidamente autorizada que ha redactado un documento clasificado; en la Comisión, los Jefes de servicio podrán autorizar a su personal a producir información clasificada de la UE;

j) «servicios de la Comisión», los distintos servicios, incluidos los gabinetes, de todos los lugares de trabajo, incluido el Centro Común de Investigación, las Representaciones y Oficinas en la Unión y las Delegaciones en países terceros.

4.3. **Clasificación**

a) En lo que atañe a la confidencialidad, se requieren cierta cautela y experiencia a la hora de seleccionar la información y el material que vayan a protegerse y evaluar el grado de protección requerido. Resulta fundamental que el grado de protección se corresponda con la importancia que revista, desde el punto de vista de la seguridad, el elemento concreto de información y material que haya de protegerse. A fin de garantizar la adecuada difusión de la información, se adoptarán las medidas necesarias para evitar una clasificación superior o inferior a la requerida.

b) El sistema de clasificación es el instrumento que permite poner en vigor estos principios. Deberá aplicarse un sistema de clasificación similar a efectos de la planificación y organización de los medios necesarios para luchar contra el espionaje, el sabotaje, el terrorismo y otras amenazas, de tal modo que se garantice la óptima protección de los locales más importantes donde se encuentre información clasificada y de los puntos más sensibles de dichos locales.

c) El único responsable de la clasificación de la información será el autor de dicha información.

d) El nivel de clasificación sólo podrá basarse en el contenido de la información.

e) En caso de que se reúnan distintas informaciones, deberá aplicarse al conjunto un nivel de clasificación al menos equivalente al nivel de clasificación más elevado. No obstante, se podrá asignar a una recopilación de informaciones una clasificación más elevada que la de sus distintos componentes.

f) La clasificación sólo se asignará en caso necesario y durante el plazo necesario.

4.4. **Objetivos de las medidas de seguridad**

Las medidas de seguridad deberán:

a) aplicarse a todas las personas que tengan acceso a información clasificada, a los soportes de información clasificada, a todos los locales en que se encuentre dicha información y a las instalaciones importantes;

b) concebirse de manera tal que permitan detectar a aquellas personas cuya posición pueda poner en peligro la seguridad de la información clasificada y de las instalaciones importantes en que se encuentre dicha información, y proceder a su exclusión o traslado;

c) impedir que personas no autorizadas tengan acceso a la información clasificada o a las instalaciones en que se encuentre dicha información;

d) garantizar que la información clasificada se difunda únicamente de conformidad con el principio de necesidad de conocer, que resulta fundamental para todos los aspectos referentes a la seguridad;

e) garantizar la integridad (es decir, impedir la alteración, la modificación o la destrucción no autorizadas) y la disponibilidad (es decir, no se denegará el acceso a las personas que necesiten la información y estén autorizadas para acceder a ella) de toda la información, clasificada o no clasificada, y, especialmente, de la información almacenada, procesada o transmitida de forma electromagnética.

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. **Normas mínimas comunes**

La Comisión garantizará la observancia de normas mínimas comunes de seguridad por parte de todos los destinatarios de información clasificada de la UE dentro de la institución y bajo su competencia, por ejemplo los servicios y contratistas, de tal modo que exista la certeza, al comunicarse la información clasificada de la UE, de que vaya a ser tratada con igual cautela. Estas normas mínimas incluirán los criterios relativos a la habilitación del personal y los procedimientos referentes a la protección de la información clasificada de la UE.

La Comisión sólo autorizará el acceso a la información clasificada de la UE a órganos externos si éstos garantizan que, al tratarse este tipo de información, se cumplan disposiciones al menos estrictamente equivalentes a las presentes normas mínimas.

5.2. **Organización**

La seguridad en la Comisión se articulará en torno a dos niveles:

a) A nivel de la Comisión en su conjunto, habrá una Oficina de Seguridad de la Comisión con una autoridad de acreditación en materia de seguridad que actuará también como autoridad Crypto y autoridad TEMPEST, y una autoridad INFOSEC, así como uno o varios registros centrales de información clasificada de la UE que contarán cada uno con uno o varios controladores de registro.

b) A nivel de los servicios de la Comisión, la seguridad será responsabilidad de uno o varios responsables locales de seguridad, uno o varios responsables centrales de seguridad informática, responsables locales de seguridad informática y registros locales de información clasificada de la UE que contarán cada uno con uno o varios controladores de registro.

c) Los órganos centrales de seguridad facilitarán orientaciones operativas a los órganos locales de seguridad.

6. SEGURIDAD DEL PERSONAL

6.1. **Habilitación del personal**

Todas las personas que necesiten acceder a la información clasificada EU CONFIDENTIAL o de nivel superior deberán someterse al debido proceso de habilitación antes de que se les autorice dicho acceso. Una habilitación similar será necesaria en el caso de las personas cuyas obligaciones impliquen la manipulación técnica o el mantenimiento de sistemas de comunicación e información que contengan información clasificada. La habilitación tendrá por objeto determinar si dichas personas:

a) son de lealtad incuestionable;

b) son de carácter y discreción tales que no arrojen ninguna duda sobre su integridad en el tratamiento de la información clasificada;

c) pueden ser sensibles a presiones externas u otras.

En los procedimientos de habilitación deberá investigarse con especial atención a las personas:

d) a las que vaya a concederse acceso a información clasificada EU TOP SECRET;

e) que ocupen puestos que conlleven el acceso habitual a un volumen considerable de información clasificada EU SECRET;

f) cuyas obligaciones les den especial acceso a sistemas de comunicación o información de seguridad y, por lo tanto, la posibilidad de obtener acceso no autorizado a un importante volumen de información clasificada de la UE, o de comprometer gravemente la misión de que se trate mediante actos de sabotaje técnico.

En las circunstancias expuestas en las letras d), e) y f), se utilizarán al máximo las técnicas de investigación de antecedentes.

Cuando haya que recurrir a personas que carezcan de una «necesidad de conocer» determinada, en circunstancias en las que puedan acceder a información clasificada de la UE (por ejemplo, mensajeros, agentes de seguridad, personal de mantenimiento y limpieza, etc.), dichas personas se someterán previamente al debido procedimiento de habilitación de seguridad.

6.2. **Registro de las habilitaciones del personal**

Todos los servicios de la Comisión que traten información clasificada de la UE o cuenten con sistemas de comunicación e información de seguridad llevarán un registro de las habilitaciones concedidas al personal que tengan asignado. Cada habilitación deberá comprobarse, en función de las circunstancias, con objeto de garantizar que resulte adecuada a la asignación de la persona en cuestión en ese momento; la habilitación deberá examinarse de nuevo con carácter prioritario siempre que se reciba nueva información indicativa de que el mantenimiento de la asignación de una persona a tareas que implican la utilización de información clasificada ha dejado de ser compatible con los intereses en materia de seguridad. El responsable local de seguridad del servicio de la Comisión llevará un registro de las habilitaciones en el sector que le corresponda.

6.3. **Instrucción del personal en materia de seguridad**

Todo el personal que trabaje en puestos en los que pueda tener acceso a información clasificada recibirá, en el momento de asumir sus funciones y a intervalos periódicos, instrucciones completas sobre las necesidades en materia de seguridad y los procedimientos aplicables a tal efecto. Deberá exigirse a este personal que certifique por escrito que ha leído y comprendido perfectamente las presentes disposiciones en materia de seguridad.

6.4. **Responsabilidades de gestión**

Los directivos tendrán la obligación de saber quiénes son los miembros de su personal que trabajan con información clasificada o tienen acceso a sistemas de comunicación e información de seguridad, así como la obligación de registrar y comunicar cuantos incidentes o aparentes muestras de vulnerabilidad puedan afectar a la seguridad.

6.5. **Situación del personal en materia de seguridad**

Deberán establecerse los procedimientos necesarios para garantizar que, cuando se den a conocer informaciones negativas en relación con una persona determinada, se determine si ésta trabaja con información clasificada o tiene acceso a sistemas de comunicación o información de seguridad y se informe a la Oficina de Seguridad de la Comisión. En caso de que se determine que representa un riesgo para la seguridad, dicha persona será excluida o cesada en las funciones en que pueda poner en peligro la seguridad.

7. SEGURIDAD FÍSICA

7.1. **Necesidad de protección**

El grado de las medidas de seguridad física que vayan a aplicarse para garantizar la protección de la información clasificada de la UE deberá ser proporcional al nivel de clasificación y al volumen de la información y del material de que se trate, así como a los riesgos a que se expongan dicha información y material. Todas las personas que estén en posesión de información clasificada de la UE deberán aplicar prácticas uniformes por lo que respecta a la clasificación de dicha información y cumplir normas comunes de protección en relación con la custodia, transmisión y eliminación de la información y del material que requieran protección.

7.2. **Comprobación**

Antes de abandonar sin vigilancia los lugares en que se encuentre información clasificada de la UE, las personas responsables de la custodia de la misma se cerciorarán de que dicha información quede almacenada de manera segura y todos los dispositivos de seguridad hayan sido activados (cerraduras, alarmas, etc.). Deberán llevarse a cabo controles independientes adicionales después de las horas de trabajo.

7.3. **Seguridad de los edificios**

Los edificios en que se encuentren información clasificada de la UE o sistemas de comunicación e información de seguridad deberán estar protegidos contra el acceso no autorizado. El tipo de protección proporcionado a la información clasificada de la UE, por ejemplo, bloqueo de ventanas, cerraduras en las puertas, guardias en las entradas, sistemas automatizados de control de acceso, controles y patrullas de seguridad, sistemas de alarma, sistemas de detección de intrusos y perros de vigilancia, dependerá de:

a) la clasificación, el volumen y la ubicación dentro del edificio de la información y del material que requieran protección,

b) la calidad de los muebles de seguridad destinados a esta información y material, y

c) la naturaleza física y la ubicación del edificio.

El tipo de protección proporcionado a los sistemas de comunicación e información dependerá asimismo de la evaluación del valor de lo que esté en juego y de los posibles daños que se derivarían en caso de peligrar la seguridad, así como de la naturaleza física y de la ubicación del edificio en que se encuentre el sistema, y de la ubicación del sistema dentro del edificio.

7.4. **Planes de emergencia**

Deberán elaborarse con antelación planes detallados para la protección de la información clasificada en caso de plantearse una situación de emergencia a escala local o nacional.

8. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información (INFOSEC) se refiere a la determinación y aplicación de medidas de seguridad para proteger la información procesada, almacenada o transmitida a través de sistemas de comunicación e información y otros sistemas electrónicos frente a la pérdida de confidencialidad, integridad o disponibilidad de la misma, ya sea accidental o intencionada. Deberán adoptarse medidas adecuadas para impedir el acceso de usuarios no autorizados a la información clasificada de la UE, impedir la denegación de acceso a este tipo de información a usuarios autorizados y la alteración, la modificación o la destrucción no autorizadas de este tipo de información.

9. LUCHA CONTRA EL SABOTAJE Y CONTROL DE OTRAS FORMAS DE DAÑO INTENCIONADO

Las precauciones físicas para la protección de instalaciones importantes en las que se encuentre información clasificada constituyen las mejores garantías de seguridad para proteger dicha información contra el sabotaje y los daños intencionados, sin que la mera habilitación del personal pueda sustituirlas de manera eficaz. Se solicitará al órgano nacional competente que facilite información confidencial relativa al espionaje, el sabotaje, el terrorismo y otras actividades subversivas.

10. DIFUSIÓN DE INFORMACIÓN CLASIFICADA A TERCEROS PAÍSES Y ORGANIZACIONES INTERNACIONALES

Corresponderá a la Comisión adoptar de forma colegiada la decisión de difundir a un país tercero u organización internacional información clasificada de la UE procedente de la Comisión. En caso de que el autor de la información que vaya a difundirse no sea la Comisión, ésta deberá recabar el consentimiento del autor de la información antes de difundirla. En caso de que no sea posible determinar el autor, la Comisión asumirá la responsabilidad del mismo.

En caso de que la Comisión reciba información clasificada procedente de terceros países, organizaciones internacionales o terceras partes, se dará a dicha información la protección adecuada a su clasificación, equivalente a las normas establecidas en las presentes disposiciones para la información clasificada de la UE o a las normas más elevadas exigidas por las terceras partes que difundan la información. Podrán disponerse controles recíprocos.

Los principios anteriormente expuestos se aplicarán con arreglo a las disposiciones establecidas en los apéndices 3, 4 y 5 de la sección 26 de la Parte II.

PARTE II: ORGANIZACIÓN DE LA SEGURIDAD EN LA COMISIÓN

11. EL MIEMBRO DE LA COMISIÓN ENCARGADO DE LA SEGURIDAD

El miembro de la Comisión encargado de la seguridad:

a) aplicará la política de seguridad de la Comisión;

b) considerará los problemas de seguridad que le transmitan la Comisión o sus órganos competentes;

c) examinará las cuestiones que impliquen cambios en la política de seguridad de la Comisión, en estrecha colaboración con las autoridades nacionales de seguridad (en lo sucesivo, «ANS») de los Estados miembros, u otras autoridades apropiadas.

En particular, corresponderá al miembro de la Comisión encargado de la seguridad:

a) coordinar todos los asuntos de seguridad relativos a las actividades de la Comisión;

b) solicitar a las autoridades designadas por los Estados miembros que las ANS faciliten habilitaciones de seguridad para el personal empleado en la Comisión, de conformidad con lo dispuesto en la sección 20;

c) investigar u ordenar que se abra una investigación sobre cualquier fuga de información clasificada de la UE de la existan indicios de que se ha producido en la Comisión;

d) pedir a las autoridades de seguridad adecuadas que abran una investigación cuando una fuga de información clasificada de la UE parezca haberse producido fuera de la Comisión, y coordinar las investigaciones en caso de que intervenga más de una autoridad de seguridad;

e) inspeccionar periódicamente las disposiciones de seguridad adoptadas para proteger la información clasificada de la UE;

f) mantener una estrecha relación con todas las autoridades de seguridad interesadas para lograr la coordinación global de la seguridad;

g) mantener bajo constante revisión la política y los procedimientos de seguridad de la Comisión y, en caso necesario, preparar las recomendaciones adecuadas; en este sentido, el miembro de la Comisión encargado de la seguridad presentará a la Comisión el plan anual de inspecciones preparado por la Oficina de Seguridad de la Comisión.

12. EL GRUPO CONSULTIVO SOBRE POLÍTICA DE SEGURIDAD DE LA COMISIÓN

Se creará un Grupo consultivo sobre política de seguridad, que estará compuesto por el miembro de la Comisión encargado de la seguridad o su delegado, que será su presidente, y por representantes de las ANS de cada Estado miembro. También podrá invitarse a representantes de otras instituciones europeas e, igualmente, podrá invitarse a representantes de los organismos descentralizados de la UE cuando se debatan cuestiones que les afecten.

El Grupo consultivo sobre política de seguridad se reunirá a instancias de su presidente o de cualquiera de sus miembros. Su cometido será examinar y evaluar todas las cuestiones de seguridad pertinentes y presentar a la Comisión las recomendaciones que procedan.

13. EL COMITÉ DE SEGURIDAD DE LA COMISIÓN

Se creará un Comité de seguridad de la Comisión, que estará compuesto por el Secretario General, que ejercerá la presidencia, y por los Directores Generales del Servicio Jurídico, de Personal y Administración, de Relaciones Exteriores, de Justicia e Interior y del Centro Común de Investigación, y por los jefes del servicio de auditoría interna de la Oficina de Seguridad de la Comisión. Podrá invitarse a otros funcionarios de la Comisión. El mandato de este Comité será examinar las medidas de seguridad existentes dentro de la Comisión y efectuar recomendaciones al respecto al miembro de la Comisión encargado de la seguridad.

14. LA OFICINA DE SEGURIDAD DE LA COMISIÓN

A fin de cumplir los cometidos indicados en la sección 11, el miembro de la Comisión encargado de la seguridad tendrá a su disposición la Oficina de Seguridad de la Comisión para coordinar, supervisar y aplicar las medidas de seguridad.

El jefe de la Oficina de Seguridad de la Comisión será el principal consejero en materia de seguridad del miembro de la Comisión encargado de la seguridad y ejercerá las funciones de secretario del Grupo consultivo sobre política de seguridad. En el cumplimiento de sus funciones, dirigirá la actualización de las normas de seguridad y coordinará las medidas de seguridad con las autoridades competentes de los Estados miembros y, cuando proceda, con las organizaciones internacionales vinculadas a la Comisión por acuerdos de seguridad. A estos efectos, actuará en calidad de funcionario de enlace.

El jefe de la Oficina de Seguridad de la Comisión será responsable de la acreditación de los sistemas y redes de tecnología de la información (en lo sucesivo, «TI») dentro de la Comisión. Tomará las decisiones, en colaboración con las ANS correspondientes, sobre la acreditación de los sistemas y redes de TI en los que participen, por un lado, la Comisión y, por otro, cualesquiera otros destinatarios de información clasificada de la UE.

15. INSPECCIONES DE SEGURIDAD

La Oficina de Seguridad de la Comisión llevará a cabo inspecciones periódicas de las disposiciones de seguridad adoptadas para proteger la información clasificada de la UE.

Para ese fin, podrá pedir la colaboración de los servicios de seguridad de las demás instituciones de la UE que traten información clasificada de la UE o de las autoridades nacionales de seguridad de los Estados miembros [1].

La ANS de un Estado miembro podrá efectuar, previa solicitud del Estado miembro, una inspección de las disposiciones de protección de la información clasificada de la UE dentro de la Comisión conjuntamente y de común acuerdo con la Oficina de Seguridad de la Comisión.

[1] Sin perjuicio del Convenio de Viena de 1961 sobre las relaciones diplomáticas y del Protocolo sobre privilegios e inmunidades de las Comunidades Europeas de 8 de abril de 1965.

16. CLASIFICACIONES, INDICACIONES Y MARCADOS DE SEGURIDAD

16.1. **Niveles de clasificación ([1])**

La información se clasificará según los siguientes niveles (véase también el apéndice 2):

EU TOP SECRET: esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros.

EU SECRET: esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda suponer un perjuicio grave para los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros.

EU CONFIDENTIAL: esta clasificación se aplicará a la información y al material cuya divulgación no autorizada pueda suponer un perjuicio para los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros.

EU RESTRICTED: esta clasificación se aplicará a la información y al material cuya divulgación no autorizada pueda resultar desventajosa para los intereses de la Unión Europea o de uno o más de sus Estados miembros.

No están permitidas otras clasificaciones.

16.2. **Indicaciones de seguridad**

Para fijar límites a la validez de una clasificación (es decir, el momento en el que se recalifica o desclasifica información clasificada) será posible utilizar una indicación de seguridad acordada. Esta indicación podrá ser «HASTA …(hora/fecha)» o «HASTA …(suceso)».

Se aplicarán indicaciones de seguridad adicionales, tales como CRYPTO o cualquier otra indicación especial de seguridad reconocida por la UE, cuando exista una necesidad de distribución limitada y de tratamiento especial además del designado por la clasificación de seguridad.

Las indicaciones de seguridad únicamente se utilizarán en combinación con una clasificación.

16.3. **Marcados**

Puede utilizarse un marcado para especificar el ámbito del documento, para indicar una difusión específica basada en el principio de necesidad de conocer o, en el caso de información no clasificada, para indicar el final de una prohibición.

Un marcado no constituye una clasificación y no puede utilizarse en lugar de la clasificación.

El marcado ESDP se aplicará a los documentos y copias de los mismos relativos a la seguridad y defensa de la Unión o de uno o más de sus Estados miembros, o referentes a la gestión militar o no militar de crisis.

16.4. **Estampación de la clasificación**

La clasificación se indicará del siguiente modo:

a) en los documentos EU RESTRICTED, por medios mecánicos o electrónicos;

b) en los documentos EU CONFIDENTIAL, por medios mecánicos, a mano, o mediante impresión en papel preestampillado y registrado;

c) en los documentos EU SECRET y EU TOP SECRET, por medios mecánicos o a mano.

16.5. **Estampación de las indicaciones de seguridad**

Las indicaciones de seguridad se estamparán debajo mismo de la clasificación del mismo modo que las clasificaciones.

([1]) En el apéndice 1 figura un cuadro comparativo de los niveles de clasificación de seguridad de la UE, de la OTAN, de la UEO y de los Estados miembros.

17. GESTIÓN DE LA CLASIFICACIÓN

17.1. **Aspectos generales**

La información sólo se clasificará cuando resulte necesario. La clasificación se indicará clara y correctamente, y se mantendrá únicamente en la medida en que la información requiera protección.

El único responsable de la clasificación de la información y de cualquier recalificación o desclasificación que se produzca posteriormente será el autor.

Los funcionarios y otros agentes de la Comisión clasificarán, recalificarán o desclasificarán la información siguiendo instrucciones de su jefe de departamento o con su consentimiento.

Los procedimientos precisos para el tratamiento de los documentos clasificados habrán sido concebidos para garantizar la protección adecuada de la información que contengan.

Se reducirá al mínimo el número de personas autorizadas a emitir documentos EU TOP SECRET y sus nombres se registrarán en una lista elaborada por la Oficina de Seguridad de la Comisión.

17.2. **Aplicación de las clasificaciones**

La clasificación de un documento se determinará con arreglo al nivel de sensibilidad de su contenido, de acuerdo con la definición de la sección 16. Es importante que la clasificación se utilice correctamente y con moderación, en particular en el caso de la clasificación EU TOP SECRET.

El autor de un documento que se vaya a clasificar deberá tener en cuenta las normas expuestas y abstenerse de clasificar de forma excesiva o insuficiente.

En el apéndice 2 figura una guía práctica de la clasificación.

Cada página, apartado, sección, anexo, apéndice o documento adjunto de un documento dado podrá requerir una clasificación diferente, lo que se indicará en consecuencia. La clasificación global del documento en su totalidad será la de la parte clasificada al nivel más alto.

La clasificación de una carta o nota de transmisión de documentos será equivalente al nivel más alto de clasificación de los documentos adjuntos. El autor deberá hacer constar claramente el nivel en que dicha carta o nota debe clasificarse cuando se separe de los documentos adjuntos.

El acceso del público seguirá rigiéndose por el Reglamento (CE) nº 1049/2001.

17.3. **Recalificación y desclasificación**

Los documentos clasificados de la UE podrán recalificarse o desclasificarse únicamente con la autorización del autor y, en caso necesario, tras consultar a las demás partes interesadas. La recalificación o desclasificación se confirmará por escrito. El autor se encargará de informar de la modificación a sus destinatarios; éstos, por su parte, se encargarán de informar de dicha modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo.

Siempre que sea posible, los autores deberán especificar en los documentos clasificados la fecha, plazo o suceso en que el contenido podrá ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años como mínimo, para comprobar si la clasificación original sigue siendo necesaria.

18. SEGURIDAD FÍSICA

18.1. **Aspectos generales**

El objetivo principal de las medidas físicas de seguridad es impedir que una persona no autorizada acceda a información o material clasificados de la UE, impedir el robo y la degradación de equipos y demás bienes, e impedir que se hostigue o agreda al personal, a otros empleados o a visitantes.

18.2. **Requisitos de seguridad**

Todos los locales, zonas, edificios, oficinas, salas, sistemas de comunicación e información, etc., en que se almacene o trate información o material clasificado de la UE se protegerán mediante las medidas de seguridad física apropiadas.

Al decidir el grado de seguridad física necesario se tendrán en cuenta todos los factores pertinentes, como:

a) la clasificación de la información o del material;

b) la cantidad y la forma (por ejemplo, copia en papel o medios de almacenamiento informáticos) de la información que se guarde;

c) la amenaza evaluada a nivel local que puedan suponer servicios de inteligencia interesados en la UE, en los Estados miembros, en otras instituciones o en terceros que posean información clasificada de la UE, con fines de, por ejemplo, sabotaje, terrorismo y otras actividades subversivas o delictivas.

Las medidas físicas de seguridad aplicadas se concebirán con vistas a:

a) impedir la entrada subrepticia o por la fuerza de intrusos;

b) disuadir, impedir y detectar actos de personal desleal;

c) impedir el acceso a información clasificada de la UE de quienes no tengan necesidad de conocer.

18.3. **Medidas físicas de seguridad**

18.3.1. *Zonas de seguridad*

Las zonas en que se trate y almacene información clasificada como EU CONFIDENTIAL o de nivel superior se organizarán y estructurarán de forma que correspondan a una de las categorías siguientes:

a) Zona de seguridad de clase I: una zona en que se trata y almacena información EU CONFIDENTIAL o de nivel superior de tal manera que la entrada en dicha zona constituye, a efectos prácticos, un acceso a información clasificada. Este tipo de zona requiere:
   i) un perímetro claramente definido y protegido en el que se controlen todas las entradas y salidas;
   ii) un sistema de control de entradas que sólo deje entrar en la zona a las personas debidamente habilitadas y especialmente autorizadas;
   iii) una especificación de la clasificación de la información que habitualmente se conserve en la zona, es decir, la información a la que se puede acceder entrando en la zona.

b) Zona de seguridad de clase II: una zona en que se trata y almacena información EU CONFIDENTIAL o de nivel superior de manera que pueda protegerse del acceso de personas no autorizadas mediante controles internos, como, por ejemplo, los locales con oficinas en las que se almacena y trata habitualmente información EU CONFIDENTIAL. Este tipo de zona requiere:
   i) un perímetro claramente definido y protegido en el que se controlen todas las entradas y salidas;
   ii) un sistema de control de entradas por el que sólo puedan entrar en la zona no acompañadas las personas debidamente habilitadas y autorizadas especialmente a acceder a la zona; para cualquier otra persona se deberá disponer la compañía de un vigilante o un control equivalente con el fin de impedir el acceso sin autorización a información clasificada de la UE y la entrada no controlada a zonas sujetas a inspecciones técnicas de seguridad.

   Las zonas no ocupadas por personal de servicio las 24 horas del día se inspeccionarán inmediatamente después del horario habitual de trabajo para cerciorarse de que la información clasificada de la UE se encuentra segura.

18.3.2. *Zona administrativa*

Se podrán crear zonas administrativas con un nivel de seguridad inferior alrededor de las zonas de seguridad de clase I y clase II, o en los espacios que conduzcan a dichas zonas. Estas zonas requerirán un perímetro definido visualmente que permita la verificación del personal y de los vehículos. En las zonas administrativas sólo se tratará y almacenará información clasificada como EU RESTRICTED e información no clasificada.

18.3.3. *Control de entradas y salidas*

Las entradas y salidas de las zonas de seguridad de clase I y clase II de todas las personas que trabajan normalmente en ellas se controlarán mediante un sistema de pases o de identificación personal. Igualmente se creará un sistema de comprobación de visitantes que impida el acceso no autorizado a la información clasificada de la UE. Los sistemas de pases podrán basarse en una identificación automatizada que se considerará adicional a los guardias, y nunca totalmente sustitutiva de éstos. Una modificación de la evaluación del riesgo podrá conllevar el refuerzo de las medidas de control de entradas y salidas, por ejemplo con motivo de la visita de personalidades.

18.3.4. *Patrullas de guardia*

Fuera del horario habitual de trabajo se realizarán patrullas por las zonas de clase I y clase II a fin de proteger el material de la UE de cualquier peligro, daño o pérdida. La frecuencia de las patrullas se determinará en función de las circunstancias locales, si bien, a título orientativo, se efectuarán cada dos horas.

18.3.5. *Mobiliario de seguridad y cámaras acorazadas*

Para almacenar información clasificada de la UE se utilizarán tres clases de muebles:

— clase A: muebles con homologación nacional para el almacenamiento de información clasificada como EU TOP SECRET en una zona de seguridad de clase I o clase II,

— clase B: muebles con homologación nacional para el almacenamiento de información clasificada como EU SECRET y EU CONFIDENTIAL en una zona de seguridad de clase I o clase II,

— clase C: mobiliario de oficina adecuado para guardar información clasificada como EU RESTRICTED únicamente.

En el caso de las cámaras acorazadas construidas dentro de una zona de seguridad de clase I o clase II y de todas las zonas de seguridad de clase I en que se almacene información EU CONFIDENTIAL y de nivel superior en estanterías abiertas o expuesta en forma de gráficos, mapas, etc., una AAS deberá certificar que las paredes, suelos y techos y puertas con cerradura ofrecen un nivel de protección equivalente al de un mueble de seguridad de la clase homologada para el almacenamiento de información de la misma clasificación.

18.3.6. *Cerraduras*

Las cerraduras utilizadas en los muebles de seguridad y las cámaras acorazadas en que se almacene información clasificada de la UE habrán de cumplir las siguientes normas:

— grupo A: homologación nacional para muebles de la clase A,

— grupo B: homologación nacional para muebles de la clase B,

— grupo C: válido únicamente para mobiliario de oficina de la clase C.

18.3.7. *Control de las llaves y las combinaciones*

Las llaves de los muebles de seguridad no se sacarán de los edificios de la Comisión. Las combinaciones de los muebles de seguridad deberán ser memorizadas por las personas que necesiten conocerlas. El responsable local de seguridad del correspondiente servicio de la Comisión tendrá bajo su custodia un juego de llaves de repuesto y un registro escrito de cada combinación, que se utilizarán en caso de emergencia. Las combinaciones se guardarán en sobres individuales opacos y sellados. Las llaves de trabajo, llaves de seguridad de repuesto y combinaciones se guardarán en muebles de seguridad aparte. Las llaves y combinaciones serán objeto de un nivel de protección de seguridad nunca inferior al del material al que den acceso.

El número de personas que conozcan las combinaciones de los muebles de seguridad será lo más limitado posible. Las combinaciones se modificarán:

a) cada vez que se reciba un nuevo mueble de seguridad;

b) cada vez que haya un cambio de personal;

c) cada vez que se produzca o se sospeche que se ha producido una situación de peligro;

d) a intervalos de seis meses, preferentemente, y como mínimo cada doce meses.

18.3.8. *Dispositivos de detección de intrusos*

Cuando se utilicen sistemas de alarma, circuitos cerrados de televisión y otros dispositivos eléctricos para proteger la información clasificada de la UE, se dispondrá de un suministro de electricidad que garantice la continuidad del funcionamiento del sistema en caso de interrupción de la alimentación eléctrica general. También es fundamental que exista una alarma u otro medio de aviso fiable al personal de vigilancia que entre en funcionamiento en caso de funcionamiento incorrecto o de intento de manipulación de los citados sistemas.

18.3.9. *Equipo homologado*

La Oficina de Seguridad de la Comisión llevará listas actualizadas, por tipos y modelos, de los equipos de seguridad que haya homologado para la protección de información clasificada en diferentes circunstancias y condiciones especificadas. Para elaborar estas listas, a Oficina de Seguridad de la Comisión se basará, entre otras fuentes, en la información facilitada por las ANS.

18.3.10. *Protección física de las fotocopiadoras y de los telefax*

Las fotocopiadoras y los telefax se protegerán físicamente en la medida necesaria para garantizar que sólo puedan ser utilizados para tratar información clasificada por personas autorizadas y que todos los productos clasificados se sometan a los debidos controles.

18.4. **Protección contra miradas y escuchas indebidas**

18.4.1. *Miradas indebidas*

Se tomarán todas las medidas adecuadas día y noche para asegurarse de que ninguna persona no autorizada vea información clasificada de la UE, así sea accidentalmente.

18.4.2. *Escuchas indebidas*

Las oficinas y zonas en que se hable habitualmente sobre información clasificada como EU SECRET o de nivel superior estarán protegidas contra la escucha pasiva y activa siempre que exista un riesgo que así lo exija. Corresponderá evaluar este riesgo a la Oficina de Seguridad de la Comisión, tras consultar, en caso necesario, a las ANS.

18.4.3. *Introducción de aparatos electrónicos y de grabación*

No se permitirá la introducción de teléfonos móviles, ordenadores personales, grabadoras, cámaras y demás aparatos electrónicos o de grabación en las zonas de seguridad o en las zonas técnicamente seguras sin autorización previa del jefe de la Oficina de Seguridad de la Comisión.

A fin de determinar las medidas de protección que han de aplicarse en los locales que puedan prestarse a escucha pasiva (por ejemplo, aislamiento de paredes, puertas, suelos y techos y medición de radiaciones sospechosas) o a escucha activa (búsqueda de micrófonos, por ejemplo), la Oficina de Seguridad de la Comisión podrá solicitar asistencia de especialistas de las ANS.

De la misma forma, cuando las circunstancias así lo exijan, el equipo de telecomunicaciones y el equipo de oficina eléctrico o electrónico de cualquier tipo que se utilice durante las reuniones a nivel EU SECRET o superior podrán someterse a comprobación por parte de especialistas técnicos en materia de seguridad de las ANS, a petición del jefe de la Oficina de Seguridad de la Comisión.

18.5. **Zonas técnicamente seguras**

Determinadas zonas podrán designarse zonas técnicamente seguras. Se efectuará un control especial de entrada a las mismas. Estas zonas se mantendrán cerradas bajo llave con un método homologado cuando no estén ocupadas y todas las llaves recibirán tratamiento de llaves de seguridad. Estas zonas se someterán a inspecciones físicas periódicas, que podrán realizarse igualmente en caso de entrada o de sospecha de entrada de personas no autorizadas.

Se realizará un inventario detallado del equipo y mobiliario a fin de seguir sus movimientos. No se introducirá en estas zonas ningún mueble o equipo que no haya sido minuciosamente inspeccionado por personal de seguridad preparado especialmente para detectar dispositivos de escucha. Como norma general, no estará permitido instalar líneas de comunicación en zonas técnicamente seguras sin autorización previa de la autoridad competente.

19. NORMAS GENERALES SOBRE EL PRINCIPIO DE NECESIDAD DE CONOCER Y LA HABILITACIÓN DE SEGURIDAD DEL PERSONAL DE LA UE

19.1. **Aspectos generales**

Únicamente estarán autorizadas a acceder a información clasificada de la UE las personas que tengan la «necesidad de conocer» por motivo de su tarea o misión. El acceso a la información clasificada EU TOP SECRET, EU SECRET y EU CONFIDENTIAL sólo se autorizará a las personas que posean la debida habilitación de seguridad.

La responsabilidad de determinar si existe la «necesidad de conocer» corresponderá al servicio en el que vaya a trabajar la persona de que se trate.

Será responsabilidad de cada servicio solicitar la habilitación de su personal.

El procedimiento desembocará en la expedición de un «certificado de seguridad» que indicará el nivel de información clasificada al que podrá acceder la persona autorizada, así como la fecha de expiración del mismo.

Un certificado de seguridad correspondiente a un nivel de clasificación determinado autorizará a su titular a acceder también a información clasificada de nivel inferior.

Las personas que no sean funcionarios u otros agentes, por ejemplo contratistas externos, expertos o consultores, con quienes haya de tratarse o a quienes haya de mostrarse información clasificada de la UE, deberán poseer una autorización de seguridad referente a información clasificada de la UE y recibir instrucciones relativas a su responsabilidad en materia de seguridad.

El acceso del público seguirá rigiéndose por el Reglamento (CE) nº 1049/2001.

19.2. **Normas específicas sobre el acceso a información clasificada como EU TOP SECRET**

Todas las personas que vayan a tener acceso a información EU TOP SECRET se someterán previamente a una comprobación de seguridad para el acceso a dicha información.

Todas las personas que necesiten acceder a información EU TOP SECRET serán designadas por el miembro de la Comisión encargado de la seguridad y su nombre figurará en el correspondiente registro EU TOP SECRET que creará y llevará la Oficina de Seguridad de la Comisión.

Antes de tener acceso a información clasificada como EU TOP SECRET, todas las personas firmarán un certificado en el que conste que han recibido instrucciones sobre los procedimientos de seguridad de la Comisión y que son plenamente conscientes de su responsabilidad especial de proteger la información EU TOP SECRET, así como de las consecuencias previstas en la normativa de la UE y en la legislación nacional o administrativa en caso de que la información clasificada pase a manos no autorizadas de manera intencional o por negligencia.

En caso de que haya personas que accedan a información EU TOP SECRET en reuniones o circunstancias similares, el controlador competente del servicio u órgano en el que trabajen dichas personas notificará al órgano que convoque la reunión que las personas mencionadas están autorizadas para ello.

Los nombres de todas las personas que dejen de desempeñar funciones para las cuales sea necesario acceder a información EU TOP SECRET se eliminarán de la lista EU TOP SECRET. Además, se recordará a dichas personas su responsabilidad especial en relación con la protección de la información EU TOP SECRET. También firmarán una declaración en la que se comprometan a no utilizar ni transmitir información clasificada como EU TOP SECRET que se encuentre en su poder.

19.3. **Normas específicas sobre el acceso a información clasificada como EU SECRET y EU CONFIDENTIAL**

Todas las personas que vayan a tener acceso a información EU SECRET o EU CONFIDENTIAL se someterán previamente a una comprobación de seguridad al nivel correspondiente.

Todas las personas que vayan a tener acceso a información EU SECRET o EU CONFIDENTIAL deberán tener conocimiento de las correspondientes normas de seguridad y conocer las consecuencias de las negligencias.

En el caso de las personas que accedan a información EU SECRET o EU CONFIDENTIAL en reuniones o circunstancias similares, el encargado de seguridad del órgano en que trabajen dichas personas notificará al órgano que convoque la reunión que dichas personas están autorizadas para ello.

19.4. **Normas específicas sobre el acceso a información clasificada como EU RESTRICTED**

Se darán a conocer a las personas con acceso a información clasificada como EU RESTRICTED las presentes normas de seguridad, así como las consecuencias de las negligencias.

19.5. **Traslados**

Cuando un miembro del personal sea trasladado de un puesto que conlleve el trabajo con material clasificado de la UE, el registro supervisará la transmisión adecuada del material del funcionario saliente al entrante.

Cuando un miembro del personal sea trasladado a otro puesto que conlleve el trabajo con material clasificado de la UE, el responsable local de seguridad le dará las instrucciones adecuadas.

19.6. **Instrucciones especiales**

Las personas que tengan que trabajar con información clasificada de la UE deberán tener conocimiento, en el momento de asumir sus tareas y periódicamente con posterioridad, de lo siguiente:

a) los peligros que entraña para la seguridad las conversaciones indiscretas;

b) las precauciones que han de tomar en sus relaciones con los medios informativos y con representantes de grupos que defienden intereses particulares;

c) la amenaza que suponen las actividades de los servicios de inteligencia que tienen como objetivo la UE y sus Estados miembros en lo relativo a la información y actividades clasificadas de la UE;

d) la obligación de informar inmediatamente a las autoridades de seguridad correspondientes sobre cualquier aproximación o maniobra sospechosa de espionaje o cualquier circunstancia anómala que afecte a la seguridad.

Todas las personas expuestas habitualmente a contactos frecuentes con representantes de países cuyos servicios de inteligencia están interesados en la información y actividades clasificadas de la UE y de los Estados miembros recibirán información sobre las técnicas que utilizan los distintos servicios de inteligencia.

No existen en la Comisión normas de seguridad referentes a los viajes privados que realiza el personal habilitado para acceder a información clasificada de la UE. No obstante, la Oficina de Seguridad de la Comisión dará a conocer a los funcionarios y otros agentes de su ámbito de responsabilidad las normas sobre viajes a las que puedan estar sujetos.

20. PROCEDIMIENTO DE HABILITACIÓN DE SEGURIDAD DE LOS FUNCIONARIOS Y OTROS AGENTES DE LA COMISIÓN

a) Sólo tendrán acceso a información clasificada que obre en poder de la Comisión los funcionarios y otros agentes de la Comisión o personas que trabajen en la misma que, por sus tareas y por necesidades del servicio, deban tener conocimiento de dicha información o utilizarla.

b) Para acceder a información clasificada como EU TOP SECRET, EU SECRET y EU CONFIDENTIAL, las personas mencionadas en la letra a) deberán haber sido autorizadas para ello con arreglo al procedimiento previsto en las letras c) y d).

c) Sólo se concederá la autorización a las personas que hayan sido sometidas a una comprobación de seguridad por las autoridades nacionales competentes de los Estados miembros (ANS) conforme al procedimiento previsto en las letras i) a n).

d) El jefe de la Oficina de Seguridad de la Comisión será el encargado de conceder las autorizaciones a que se refieren las letras a), b) y c).

e) Concederá la autorización tras recabar el dictamen de las autoridades nacionales competentes de los Estados miembros sobre la base de la comprobación de seguridad efectuada de acuerdo con las letras i) a n).

f) La Oficina de Seguridad de la Comisión llevará una lista actualizada de todos los puestos sensibles, comunicados por los correspondientes servicios de la Comisión, y de todas las personas que hayan recibido una autorización (temporal).

g) La autorización, que será válida durante un período de cinco años, no podrá sobrepasar la duración de las tareas que motivaron su concesión. Podrá ser renovada de acuerdo con el procedimiento indicado en la letra e).

h) El jefe de la Oficina de Seguridad de la Comisión retirará la autorización si considera que existen motivos para ello. La decisión de retirar la autorización se notificará al interesado, que podrá solicitar ser oído por el jefe de la Oficina de Seguridad de la Comisión, y a la autoridad nacional competente.

i) La comprobación de seguridad se realizará con la asistencia del interesado y a instancias del jefe de la Oficina de Seguridad de la Comisión. La autoridad nacional competente será la del Estado miembro del que sea nacional el interesado. Si éste no es un nacional de un Estado miembro de la UE, el jefe de la Oficina de Seguridad de la Comisión solicitará una comprobación de seguridad sobre él al Estado miembro en el que esté domiciliado o resida habitualmente.

j) En el marco del procedimiento de comprobación de seguridad, se pedirá al interesado que cumplimente una ficha personal de información.

k) El jefe de la Oficina de Seguridad de la Comisión especificará en su solicitud el tipo y el nivel de información clasificada al que tendrá acceso el interesado, de manera que las autoridades nacionales competentes puedan llevar a cabo la comprobación de seguridad y dar su opinión sobre el nivel de autorización que sería adecuado conceder a dicha persona.

l) El conjunto del procedimiento de comprobación de seguridad, junto con los resultados obtenidos, se regirán por la normativa vigente en el Estado miembro interesado, incluida la relativa a los recursos.

m) Si las autoridades nacionales competentes de Estado miembro emiten un dictamen positivo, el jefe de la Oficina de Seguridad de la Comisión podrá conceder la autorización al interesado.

n) Si el dictamen es negativo, las autoridades nacionales competentes lo notificarán al interesado, que podrá solicitar ser oído por el jefe de la Oficina de Seguridad de la Comisión. Si lo considera necesario, el jefe de la Oficina de Seguridad de la Comisión podrá solicitar a las autoridades nacionales competentes cualquier otra aclaración que puedan facilitar. En caso de que se confirme el dictamen negativo, no se concederá la autorización.

o) Todas las personas a las que se conceda autorización con arreglo a las letras d) y e) recibirán, en el momento en que se conceda la autorización y a intervalos regulares posteriormente, todas las instrucciones necesarias sobre la protección de la información clasificada y sobre los medios para garantizar dicha protección. Estas personas firmarán una declaración en la que declaren que conocen las instrucciones y se comprometen a respetarlas.

p) El jefe de la Oficina de Seguridad de la Comisión adoptará cuantas medidas considere necesarias para aplicar la presente sección, en particular en lo relativo a las normas por las que se rige el acceso a la lista de personas autorizadas.

q) A título excepcional, en caso de que el servicio lo exija, el jefe de la Oficina de Seguridad de la Comisión podrá conceder una autorización temporal, previa notificación a las autoridades nacionales competentes y siempre que éstas no respondan en el plazo de un mes, para un período que no superará los seis meses, en espera del resultado de la comprobación de seguridad prevista en la letra i).

r) Las autorizaciones provisionales y temporales concedidas de esta forma no darán acceso a información clasificada como EU TOP SECRET; sólo podrán acceder a esta información los funcionarios que hayan superado con éxito una comprobación de seguridad, con arreglo a lo previsto en la letra i). En espera del resultado de la comprobación de seguridad, los funcionarios para los que se ha solicitado una autorización de nivel EU TOP SECRET podrán ser autorizados con carácter temporal y provisional a acceder a información clasificada hasta el nivel EU SECRET inclusive.

21. ELABORACIÓN, DIFUSIÓN, TRANSMISIÓN, SEGURIDAD DEL PERSONAL DE CORREO, COPIAS ADICIONALES, TRADUCCIONES Y EXTRACTOS DE DOCUMENTOS CLASIFICADOS DE LA UE

21.1. **Elaboración**

1. Las clasificaciones de la UE se aplicarán según lo establecido en la sección 16. En los documentos EU CONFIDENTIAL y de nivel superior, la clasificación figurará en la parte central, superior e inferior, de cada página. Todas las páginas irán numeradas. Todos los documentos clasificados de la UE llevarán un número de referencia y una fecha. En el caso de los documentos EU TOP SECRET y EU SECRET, el número de referencia aparecerá en cada página. Si se han de distribuir varias copias, cada una de ellas llevará un número de copia, que figurará en la primera página, junto con la indicación del número total de páginas. En los documentos clasificados como EU CONFIDENTIAL y de nivel superior, todos los anexos y documentos adjuntos se indicarán en la primera página.

2. Los documentos clasificados como EU CONFIDENTIAL y de nivel superior serán mecanografiados, traducidos, almacenados, fotocopiados, reproducidos magnéticamente o microfilmados únicamente por personas autorizadas para acceder a información clasificada de la UE como mínimo hasta el nivel de clasificación de seguridad correspondiente al documento de que se trate.

3. Las disposiciones por las que se rige la producción informatizada de documentos clasificados figuran en la sección 25.

21.2. **Difusión**

1. Únicamente se difundirá información clasificada de la UE a las personas que tengan necesidad de conocerla y posean la debida habilitación de seguridad. El autor especificará la lista inicial de difusión.

2. La difusión de documentos clasificados como EU TOP SECRET se efectuará a través de registros EU TOP SECRET (véase sección 22.2). En el caso de los mensajes EU TOP SECRET, el registro competente podrá autorizar al jefe del centro de comunicaciones a realizar el número de copias indicado en la lista de destinatarios.

3. Los documentos clasificados como EU SECRET y de nivel inferior podrán ser difundidos a su vez por los destinatarios iniciales a otros destinatarios. No obstante, las autoridades autoras podrán hacer constar cualquier tipo de restricción que deseen imponer. Cuando se impongan estas restricciones, los destinatarios sólo podrán difundir los documentos con la autorización de las autoridades autoras.

4. A la entrada o salida de una Dirección General o Servicio, los documentos clasificados como EU CONFIDENTIAL y de nivel superior se inscribirán en el registro local de información clasificada de la UE del servicio de que se trate. Se anotarán pormenores (referencias, fecha y, en su caso, número de copia) que permitan identificar los documentos y se incluirán en un registro o en un soporte informatizado especialmente protegido (véase sección 22.1).

21.3. **Transmisión de documentos clasificados de la UE**

21.3.1. *Pliegos y acuses de recibo*

1. Los documentos clasificados como EU CONFIDENTIAL y de nivel superior se transmitirán en doble pliego mediante sobres opacos y de gran resistencia. El sobre interior irá marcado con la correspondiente clasificación de seguridad de la UE y, si es posible, con indicación completa del cargo del destinatario y de su dirección.

2. Únicamente un controlador de registro (véase sección 22.1), o su sustituto, podrán abrir el sobre interior y acusar recibo de los documentos adjuntos, salvo que el sobre vaya dirigido a una persona concreta. En este caso, se hará constar en el registro correspondiente (véase sección 22.1) la llegada del sobre, y únicamente la persona a la que éste vaya destinado podrá abrir el sobre interior y acusar recibo de los documentos que contenga.

3. El sobre interior contendrá un impreso de acuse de recibo, que no estará clasificado y en el que figurarán el número de referencia, la fecha y el número de copia del documento, pero nunca la materia de que trate.

4. El sobre interior irá dentro de un sobre exterior en el que se indicará el número de envío a efectos de recepción. Bajo ningún concepto figurará la clasificación de seguridad en el sobre exterior.

5. En el caso de los documentos clasificados como EU CONFIDENTIAL o de nivel superior, los correos y mensajeros recibirán impresos de acuse de recibo que correspondan al número de envío.

21.3.2. *Transmisión dentro de un edificio o grupo de edificios*

Dentro de un edificio o grupo de edificios dado, los documentos clasificados podrán ser transportados en un sobre sellado que lleve únicamente el nombre del destinatario, a condición de que la persona que los transporte posea una habilitación equivalente al nivel de clasificación de los documentos.

21.3.3. *Transmisión dentro de un país*

1. Dentro de un país, los documentos clasificados como EU TOP SECRET deberán enviarse únicamente a través de un servicio de mensajería oficial o de personas autorizadas para acceder a información clasificada como EU TOP SECRET.

2. Cada vez que se recurra a un servicio de mensajería para la transmisión de un documento EU TOP SECRET fuera de los límites físicos de un edificio o grupo de edificios, se aplicarán las disposiciones en materia de pliegos y recepción que figuran en el presente capítulo. La dotación de personal de los servicios de reparto será tal que los paquetes que contengan documentos EU TOP SECRET permanezcan en todo momento bajo la supervisión directa de un funcionario en el que recaiga la responsabilidad.

3. Excepcionalmente, funcionarios que no sean mensajeros podrán llevar documentos clasificados como EU TOP SECRET fuera de los límites físicos de un edificio o grupo de edificios, para uso local en reuniones y deliberaciones, siempre que se cumplan las siguientes condiciones:

   a) el portador esté autorizado a acceder a esos documentos EU TOP SECRET;

   b) el modo de transporte cumpla las normas que regulan la transmisión de documentos clasificados como EU TOP SECRET;

   c) el funcionario no se separe de los documentos EU TOP SECRET en ningún momento;

   d) se tomen disposiciones para que en el registro EU TOP SECRET en el que se conservan los documentos figure la lista de documentos así transportados, se anoten éstos en un registro y se compruebe su devolución.

4. Dentro de un país dado, los documentos EU SECRET y EU CONFIDENTIAL podrán enviarse bien por correo, si esta transmisión está autorizada por las normas nacionales y cumple lo dispuesto por ellas, bien mediante un servicio de mensajería, bien por personas autorizadas a acceder a información clasificada de la UE.

5. La Oficina de Seguridad de la Comisión dictará instrucciones para el personal que transporte documentos clasificados de la UE que se basarán en las presentes normas. El portador estará obligado a leer y firmar dichas instrucciones. En particular, las instrucciones deberán dejar claro que bajo ningún concepto los documentos podrán:

   a) dejar de estar en posesión del portador, a menos que estén bajo custodia segura, conforme a lo dispuesto en la sección 18;

   b) quedar descuidados en transportes públicos o en vehículos privados, o en lugares como restaurantes u hoteles; no podrán guardarse en cajas fuertes de hotel ni quedar descuidados en habitaciones de hotel;

   c) leerse en lugares públicos, como aviones o trenes.

21.3.4. *Transmisión de un Estado a otro*

1. El material clasificado como EU CONFIDENTIAL y de nivel superior será expedido a través del servicio de correo diplomático o militar.

2. No obstante, podrá permitirse el transporte personal de material clasificado como EU SECRET y EU CONFIDENTIAL si las disposiciones relativas a su transporte garantizan que no caiga en manos de personas no autorizadas.

3. El miembro de la Comisión encargado de la seguridad podrá autorizar el transporte personal cuando no se disponga de correos diplomáticos o militares o el recurso a los mismos pueda producir un retraso perjudicial para el funcionamiento de la UE y el destinatario previsto necesite con urgencia el material. La Oficina de Seguridad de la Comisión dictará instrucciones relativas al transporte personal de material clasificado hasta el nivel EU SECRET inclusive por personas que no sean correos diplomáticos o militares. Dichas instrucciones deberán exigir lo siguiente:

   a) el portador deberá tener la habilitación de seguridad adecuada;

   b) se anotará el material así transportado en la oficina o registro correspondiente;

   c) los paquetes o bolsas que contengan material de la UE llevarán un sello oficial para impedir o disuadir de la inspección por los aduaneros, así como etiquetas con identificación e instrucciones para la persona que los encuentre;

   d) el portador llevará un certificado de correo u orden de misión reconocidos por todos los Estados miembros de la UE que lo autoricen a llevar el paquete identificado;

   e) cuando se viaje por tierra no se atravesará un Estado que no sea miembro de la UE ni se cruzará su frontera, a menos que el Estado de expedición tenga garantías específicas de ese Estado;

   f) todas las disposiciones para el viaje del portador en lo relativo a los destinos, rutas que se vayan a seguir y medios de transporte que se vayan a utilizar se ajustarán a las normas de la UE o, si las normas nacionales en este ámbito son más estrictas, a estas últimas;

g) el material nunca podrá dejar de estar en posesión del portador a menos que se proteja de acuerdo con las disposiciones en materia de custodia de seguridad que figuran en la sección 18;

h) el material nunca podrá quedar descuidado en vehículos públicos o privados, o en lugares como restaurantes u hoteles; o deberá guardarse en cajas fuertes de hotel o quedar descuidado en habitaciones de hotel;

i) en caso de que el material transportado contenga documentos, éstos no deberán leerse en lugares públicos (aviones, trenes, etc.).

4. La persona designada para transportar el material clasificado deberá leer y firmar unas consignas de seguridad que contengan, como mínimo, las instrucciones antes expuestas y los procedimientos que se deberán seguir en caso de emergencia o cuando el paquete sea detenido por aduaneros o agentes de seguridad de aeropuerto.

21.3.5. *Transmisión de documentos clasificados como EU RESTRICTED*

No se establecen medidas especiales para el envío de documentos clasificados como EU RESTRICTED, salvo que el envío debe efectuarse de tal forma que dichos documentos no caigan en manos de personas no autorizadas.

21.4. **Seguridad del personal de correo**

Todos los correos y mensajeros utilizados para llevar documentos clasificados como EU SECRET o EU CONFIDENTIAL habrán de tener la debida habilitación de seguridad.

21.5. **Medios técnicos de transmisión electrónicos y otros**

1. Las medidas de seguridad de las comunicaciones estarán concebidas para garantizar la transmisión segura de información clasificada de la UE. En la sección 25 figuran las normas detalladas aplicables a la transmisión de dicha información clasificada de la UE.

2. Únicamente los centros y redes o terminales y sistemas de comunicación acreditados podrán transmitir información clasificada como EU CONFIDENTIAL o EU SECRET.

21.6. **Copias adicionales, traducciones y extractos de documentos clasificados de la UE**

1. Sólo el autor podrá autorizar la copia o traducción de documentos clasificados como EU TOP SECRET.

2. Si personas sin habilitación EU TOP SECRET necesitan información que, a pesar de figurar en un documento EU TOP SECRET, no tiene dicha clasificación, el jefe del registro EU TOP SECRET (véase sección 22.2) podrá ser autorizado a efectuar la cantidad necesaria de extractos de dicho documento. Al mismo tiempo, hará lo necesario para garantizar que dichos extractos reciban la clasificación de seguridad adecuada.

3. Los documentos clasificados como EU SECRET o de nivel inferior podrán ser reproducidos y traducidos por el destinatario, dentro del marco de las presentes normas de seguridad y con la condición de que cumpla estrictamente con el principio de necesidad de conocer. Las medidas de seguridad aplicables a los documentos originales serán también aplicables a las reproducciones o traducciones del mismo.

22. REGISTROS, COLECCIONES, CONTROLES, ALMACENAMIENTO EN ARCHIVOS Y DESTRUCCIÓN DE INFORMACIÓN CLASIFICADA DE LA UE

22.1. **Registros locales de información clasificada de la UE**

1. En cada servicio de la Comisión, según proceda, uno o más registros locales de información clasificada de la UE se encargarán del registro, reproducción, envío, archivo y destrucción de documentos clasificados EU SECRET o EU CONFIDENTIAL.

2. Cuando un servicio no disponga de un registro local de información clasificada de la UE, el registro local de información clasificada de la UE de la Secretaría General cumplirá esa función.

3. Los registros locales de información clasificada de la UE dependerán del jefe de servicio del que reciben instrucciones. El jefe de estos registros será el controlador del registro.

4. Los registros locales de información clasificada de la UE serán supervisados por el responsable local de seguridad en lo relativo a la aplicación de las disposiciones sobre el tratamiento de los documentos de información clasificada de la UE y el cumplimiento de las correspondientes medidas de seguridad.

5. Los funcionarios asignados a los registros locales de información clasificada de la UE estarán autorizados para poder acceder a la información clasificada de la UE de conformidad con la sección 20.

6. Bajo la autoridad del jefe de servicio pertinente, los registros locales de información clasificada de la UE:

   a) controlarán las operaciones relativas al registro, reproducción, traducción, envío y destrucción de dicha información;

   b) actualizarán el registro de información clasificada;

   c) periódicamente se interrogarán sobre la necesidad de mantener la clasificación de la información.

7. Los registros locales de información clasificada de la UE mantendrán un registro con la siguiente información:

   a) la fecha de elaboración de la información clasificada;

   b) el nivel de clasificación;

   c) la fecha en que expira la clasificación;

   d) el nombre y el servicio del autor;

   e) el destinatario o destinatarios, con el número de serie;

   f) el asunto;

   g) el número;

   h) el número de ejemplares distribuidos;

   i) la elaboración de inventarios de la información clasificada transmitida al servicio;

   j) el registro de desclasificación o recalificación de información clasificada.

8. Las normas generales establecidas en la sección 21 se aplicarán a los registros locales de información clasificada de la UE de la Comisión, a menos que se modifiquen mediante las normas específicas establecidas en la presente sección.

22.2. **Registro EU TOP SECRET**

22.2.1. *Aspectos generales*

1. Un registro central EU TOP SECRET garantiza el almacenamiento, tratamiento y distribución de documentos EU TOP SECRET con arreglo a las presentes disposiciones de seguridad. El jefe del registro EU TOP SECRET será el controlador EU TOP SECRET.

2. El registro central EU TOP SECRET actuará como la principal autoridad receptora y emisora de los Estados miembros, con otras instituciones de la UE, Estados miembros, organizaciones internacionales y terceros Estados con los que la Comisión tenga acuerdos sobre procedimientos de seguridad para el intercambio de información clasificada.

3. Cuando sea necesario, se establecerán registros secundarios encargados de la gestión interna de los documentos EU TOP SECRET, que mantendrán datos actualizados sobre la circulación de cada documento a cargo del registro secundario.

4. Los registros secundarios EU TOP SECRET se crearán según lo dispuesto en la sección 22.2.3 en respuesta a las necesidades a largo plazo y estarán vinculados a un registro central EU TOP SECRET. Si hay necesidad de consultar documentos EU TOP SECRET sólo temporal y ocasionalmente, estos documentos podrán darse a conocer sin crear un registro secundario EU TOP SECRET, siempre que se establezcan normas para garantizar que permanecen bajo control del registro EU TOP SECRET pertinente y que se observan todas las normas de seguridad físicas y de personal.

5. Los registros secundarios no transmitirán documentos EU TOP SECRET directamente a otros registros secundarios del mismo registro central EU TOP SECRET sin la expresa aprobación de este último.

6. Todos los intercambios de documentos EU TOP SECRET entre registros secundarios que no dependan del mismo registro central se tramitarán a través de los registros centrales EU TOP SECRET.

22.2.2. *Registro central EU TOP SECRET*

En su calidad de controlador, el jefe del registro central EU TOP SECRET se encargará de:

a) transmitir los documentos EU TOP SECRET con arreglo a lo dispuesto en la sección 21.3;

b) mantener una lista de todos sus registros secundarios dependientes EU TOP SECRET, junto con los nombres y firmas de los controladores designados y de sus suplentes autorizados;

c) guardar recibos de los registros de todos los documentos EU TOP SECRET distribuidos por el registro central;

d) mantener un registro de los documentos EU TOP SECRET guardados y distribuidos;

e) mantener una lista actualizada de todos los registros centrales EU TOP SECRET con los que normalmente mantiene correspondencia, junto con los nombres y firmas de sus controladores designados y de sus suplentes autorizados;

f) velar por la protección física de todos los documentos EU TOP SECRET del registro con arreglo a las normas de la sección 18.

22.2.3. *Registros secundarios EU TOP SECRET*

En su calidad de controlador, el jefe de un registro secundario EU TOP SECRET se encargará de:

a) transmitir los documentos EU TOP SECRET con arreglo a lo dispuesto en la sección 21.3;

b) mantener una lista actualizada de todas las personas autorizadas a tener acceso a la información EU TOP SECRET bajo su control;

c) distribuir los documentos EU TOP SECRET con arreglo a las instrucciones del autor o según la necesidad de conocer, comprobando en primer lugar que el destinatario tiene la habilitación de seguridad exigida;

d) mantener un registro actualizado de todos los documentos EU TOP SECRET guardados o en circulación bajo su control o que hayan pasado por otros registros EU TOP SECRET y guardar todos los recibos correspondientes;

e) mantener una lista actualizada de los registros EU TOP SECRET con los que está autorizado a intercambiar documentos clasificados EU TOP SECRET, junto con los nombres y firmas de los controladores designados y de sus suplentes autorizados;

f) velar por la protección física de todos los documentos EU TOP SECRET del registro secundario con arreglo a las normas de la sección 18.

22.3. **Inventarios, colecciones y controles de documentos clasificados de la UE**

1. Anualmente, cada registro EU TOP SECRET a que se refiere la presente sección llevará a cabo un inventario detallado de los documentos EU TOP SECRET. Se considerará que se ha respondido de un documento si el registro cuenta físicamente con él, o guarda un recibo del registro EU TOP SECRET al que se ha enviado, un certificado de su destrucción o una instrucción de recalificación o desclasificación de dicho documento. Los registros presentarán los resultados de los inventarios anuales al miembro de la Comisión encargado de la seguridad, a más tardar el 1 de abril de cada año.

2. Los registros secundarios EU TOP SECRET presentarán los resultados de su inventario anual al registro central ante el que son responsables, en la fecha que determine este último.

3. Los documentos clasificados de la UE de una categoría inferior a la de EU TOP SECRET se someterán a controles internos de acuerdo con las instrucciones del miembro de la Comisión encargado de la seguridad.

4. Estas operaciones permitirán afianzar la opinión de los poseedores sobre:

   a) la posibilidad de recalificar o desclasificar determinados documentos;

   b) los documentos que deben destruirse.

22.4. **Almacenamiento en archivos de información clasificada de la UE**

1. La información clasificada de la UE deberá almacenarse en condiciones que cumplan todos los requisitos pertinentes que se enumeran en la sección 18.

2. Para reducir al mínimo los problemas de almacenamiento, los controladores de todos los registros estarán autorizados para microfilmar los documentos EU TOP SECRET, EU SECRET y EU CONFIDENTIAL o para guardarlos en medios magnéticos u ópticos con objeto de archivarlos, siempre y cuando:

   a) el proceso de microfilmado o almacenamiento lo realice personal con habilitación vigente para el nivel de clasificación apropiado correspondiente;

   b) el medio de microfilmado o almacenamiento goce de la misma seguridad que los documentos originales;

   c) se informe al autor sobre el microfilmado o almacenamiento de todo documento EU TOP SECRET;

   d) los carretes de fotos u otro tipo de soporte contengan sólo documentos de la misma clasificación EU TOP SECRET, EU SECRET o EU CONFIDENTIAL;

   e) el microfilmado o almacenamiento de un documento EU TOP SECRET o EU SECRET aparezca claramente indicado en el registro utilizado para el inventario anual;

   f) los documentos originales que se hayan microfilmado o almacenado de otro modo se destruyan con arreglo a las normas establecidas en la sección 22.5.

3. Estas normas se aplicarán también a cualquier otra forma de almacenamiento autorizado, como los medios electromagnéticos o los discos ópticos.

22.5. **Destrucción de documentos clasificados de la UE**

1. Para evitar una acumulación innecesaria de documentos clasificados de la UE, los que, a juicio del jefe de la organización que los tenga en su poder, sean anticuados y excesivos en número se destruirán tan pronto como sea posible de la manera siguiente:

   a) Los documentos EU TOP SECRET sólo los destruirá el registro central encargado de su custodia. Los documentos destruidos se enumerarán en un certificado de destrucción, firmado por el controlador EU TOP SECRET y por el funcionario que haya presenciado la destrucción, que tendrá la habilitación EU TOP SECRET. En el libro de registro se hará una anotación al efecto.

   b) El registro conservará los certificados de destrucción, junto con los impresos de distribución, durante diez años. Sólo cuando se solicite expresamente se transmitirán copias al autor o al registro central que corresponda.

   c) Los documentos EU TOP SECRET, incluidos todos los restos de documentos clasificados que se hayan utilizado para preparar documentos EU TOP SECRET, como copias defectuosas, borradores de trabajo, notas mecanografiadas y disquetes, se destruirán, bajo la supervisión de un controlador de registro EU TOP SECRET, quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles y no puedan reconstituirse.

2. Los documentos EU SECRET los destruirá el registro encargado de su custodia, bajo la supervisión de una persona con habilitación de seguridad, utilizando uno de los procesos indicados en la letra c) del apartado 1. Los documentos EU SECRET que se destruyan se incluirán en certificados de destrucción firmados que se guardarán en el registro, junto con los impresos de distribución, durante al menos tres años.

3. Los documentos EU CONFIDENTIAL los destruirá el registro encargado de su custodia, bajo la supervisión de una persona con habilitación de seguridad, utilizando uno de los procesos indicados en la letra c) del apartado 1. Se guardará constancia de su destrucción con arreglo a las instrucciones del miembro de la Comisión encargado de la seguridad.

4. Los documentos EU RESTRICTED los destruirá el registro encargado de su custodia o el usuario, con arreglo a las instrucciones del miembro de la Comisión encargado de la seguridad.

22.6. **Destrucción en situaciones de urgencia**

1. Los servicios de la Comisión 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. Asimismo, promulgarán las instrucciones que se estimen necesarias para impedir que la información clasificada de la UE caiga en manos de personas no autorizadas.

2. Las disposiciones para la protección o la destrucción de material EU SECRET y EU CONFIDENTIAL en situaciones de crisis no afectarán en ningún caso a la protección o destrucción de material EU TOP SECRET, incluido el equipo de mensajes cifrados, cuyo tratamiento deberá tener prioridad sobre todas las demás tareas.

3. Las medidas que deban adoptarse para la protección y destrucción del equipo de mensajes cifrados en una situación de urgencia figurarán en instrucciones específicas.

4. Será necesario disponer de instrucciones *in situ* en un sobre cerrado. Asimismo deberá contarse con medios o instrumentos de destrucción.

23. MEDIDAS DE SEGURIDAD APLICABLES A LAS REUNIONES ESPECÍFICAS CELEBRADAS FUERA DE LOS LOCALES DE LA COMISIÓN EN LAS QUE SE UTILICE INFORMACIÓN CLASIFICADA DE LA UE

23.1. **Aspectos generales**

Cuando las reuniones de la Comisión u otras reuniones importantes se celebren fuera de los locales de la Comisión y cuando los requisitos específicos de seguridad relativos a la gran sensibilidad de los temas tratados o de la información utilizada así lo justifiquen, deberán adoptarse las medidas de seguridad descritas a continuación. Estas medidas afectan únicamente a la protección de información clasificada de la UE, por lo que tal vez sea necesario preparar otras medidas de seguridad.

23.2. **Atribuciones**

23.2.1. *Oficina de Seguridad de la Comisión*

La Oficina de Seguridad de la Comisión deberá cooperar con las autoridades competentes del Estado miembro en cuyo territorio se celebre la reunión (el Estado miembro anfitrión) con el fin de garantizar la seguridad de las reuniones de la Comisión o de otras reuniones importantes, así como la seguridad física de los delegados y de su personal. Con respecto a la protección de la seguridad, deberá concretamente garantizar que:

a) se elaboran planes para hacer frente a amenazas de la seguridad e incidentes relacionados con la seguridad; las medidas en cuestión abarcarán en particular la custodia segura de documentos clasificados de la UE en los despachos;

b) se adoptan medidas para proporcionar un posible acceso al sistema de comunicaciones de la Comisión para la recepción y transmisión de mensajes clasificados de la UE; se pedirá al Estado miembro anfitrión que proporcione acceso a sistemas de telefonía de seguridad, si así se solicita.

La Oficina de Seguridad de la Comisión deberá actuar como órgano consultor de seguridad para la preparación de la reunión; deberá estar representada *in situ* para ayudar y aconsejar al responsable de seguridad de la reunión y a las delegaciones, si fuera necesario.

Cada una de las delegaciones de una reunión deberá designar un agente de seguridad que se ocupará de la seguridad en su delegación y de mantener contactos con el responsable de seguridad de la reunión, así como con el representante de la Oficina de Seguridad de la Comisión, si fuera necesario.

23.2.2. *Responsable de seguridad de reunión*

Deberá nombrarse un responsable de seguridad de reunión que se encargará, en general, de la preparación y del control de las medidas generales de seguridad interna y de la coordinación con las demás autoridades de seguridad en cuestión. Las medidas adoptadas por dicho agente se referirán en general a lo siguiente:

a) medidas de protección en el lugar donde se celebre la reunión para garantizar que esta se desarrolla sin incidentes que puedan poner en peligro la seguridad de cualquier información clasificada de la EU que pueda utilizarse;

b) el control del personal autorizado a acceder al lugar donde se celebre la reunión, a las zonas destinadas a las delegaciones y a las salas de conferencia, y el control de todo el equipo;

c) una coordinación constante con las autoridades competentes del Estado miembro anfitrión y con la Oficina de Seguridad de la Comisión;

d) la inclusión de instrucciones de seguridad en la documentación de la reunión, teniendo en cuenta los requisitos establecidos en las presentes normas y cualquier otra instrucción de seguridad que se considere necesaria.

23.3. **Medidas de seguridad**

23.3.1. *Zonas de seguridad*

Se crearán las siguientes zonas de seguridad:

a) una zona de seguridad de clase II, constituida por una sala de redacción, los despachos de la Comisión y su equipo de reprografía y los despachos de las delegaciones, según convenga;

b) una zona de seguridad de clase I, constituida por la sala de conferencias y las cabinas de sonido y de interpretación;

c) las zonas administrativas, constituidas por la zona de prensa y las partes del local de la reunión utilizadas para la administración, la comida y el alojamiento, así como la zona inmediatamente contigua al centro de prensa y al lugar de la reunión.

23.3.2. *Pases*

El responsable de seguridad de reunión deberá suministrar las tarjetas adecuadas que soliciten las delegaciones, según sus necesidades. Siempre que sea necesario, podrá distinguirse entre el acceso a las diferentes zonas de seguridad.

Las instrucciones de seguridad de la reunión deberán exigir que todos los participantes ostenten de forma visible y permanente sus tarjetas mientras se encuentren en el lugar de la reunión, para que el personal de seguridad pueda controlarlas según se requiera.

Aparte de los participantes con tarjeta, deberá reducirse al mínimo el número de personas que pueden entrar en el lugar de la reunión. El responsable de seguridad de reunión sólo permitirá que las delegaciones nacionales reciban visitantes durante la reunión si lo solicitan previamente. Cada visitante dispondrá de una tarjeta y se deberá rellenar un formulario de entrada con su nombre y el nombre de la persona objeto de la visita. Los visitantes permanecerán siempre acompañados de un guardia de seguridad o de la persona objeto de la visita. Cuando el visitante abandone el lugar de la reunión, la persona que lo acompañe deberá entregar su formulario, junto con la tarjeta de visitante, al personal de seguridad.

23.3.3. *Control de los equipos de fotografía y sonido*

En las zonas de seguridad de clase I no podrá entrar ninguna cámara o equipo de grabación más que el empleado por los fotógrafos y los ingenieros de sonido debidamente autorizados por el responsable de seguridad de reunión.

23.3.4. *Control de maletines, ordenadores portátiles y paquetes*

Las personas que tengan un pase con acceso a una zona de seguridad en general podrán llevar sus maletines y ordenadores portátiles (sólo con alimentación independiente) sin que se efectúe control alguno. Los paquetes dirigidos a las delegaciones podrán serán recogidos por éstas y deberán ser comprobados por el agente de seguridad de la delegación, inspeccionados mediante aparatos especiales o abiertos por el personal de seguridad. Si el responsable de seguridad de reunión lo considera necesario, podrán establecerse medidas más estrictas de inspección de maletines y paquetes.

23.3.5. *Seguridad técnica*

Un equipo de seguridad técnica se encargará de que la sala de reuniones sea técnicamente segura y también podrá llevar a cabo un control electrónico durante la reunión.

23.3.6. *Documentos de las delegaciones*

Las delegaciones se encargarán de llevar y traer los documentos clasificados de la UE a las reuniones. También deberán encargarse del control y la seguridad de esos documentos mientras los utilicen en los locales que se les asignen. Podrá solicitarse ayuda del Estado miembro anfitrión para llevar y traer los documentos clasificados al lugar donde se celebre la reunión.

23.3.7. *Custodia segura de los documentos*

Si la Comisión o las delegaciones no pudieran guardar sus documentos clasificados de conformidad con las normas establecidas, podrán entregarlos en un sobre cerrado al responsable de seguridad de reunión, contra entrega del recibo pertinente, para que éste pueda guardarlos según las normas establecidas.

23.3.8. *Control de los despachos*

El responsable de seguridad de reunión dispondrá que, al término de cada jornada de trabajo, se realice una inspección de los despachos de la Comisión y de las delegaciones para garantizar que todos los documentos clasificados de la UE están en un lugar seguro. Si no fuera así, tomará las medidas oportunas.

23.3.9. *Eliminación de los restos de documentos clasificados de la UE*

Todos los restos de documentos se considerarán material clasificado de la UE. Deberán entregarse papeleras y bolsas a la Comisión y a las delegaciones para que recojan los papeles. Antes de abandonar los locales que se les hayan asignado, la Comisión y las delegaciones deberán entregar los papeles al responsable de seguridad de la reunión, que ordenará su destrucción según las normas.

Al final de la reunión, todos los documentos que la Comisión o las delegaciones ya no deseen se tratarán como restos de documentos. Antes de levantar las medidas de seguridad decretadas para la reunión se llevará a cabo un registro exhaustivo de los locales utilizados por la Comisión y por las delegaciones. En la medida de lo posible, los documentos que se hayan entregado a cambio de un recibo se destruirán de conformidad con lo dispuesto en la sección 22.5.

24. INFRACCIONES DE LA SEGURIDAD Y RIESGO A QUE SE EXPONE LA INFORMACIÓN CLASIFICADA DE LA UE

24.1. **Definiciones**

Infringir la seguridad es un acto u omisión contrario a una norma de seguridad de la Comisión que puede poner en peligro o exponer a riesgo información clasificada de la UE.

La información clasificada de la UE se expone a riesgo cuando cae total o parcialmente en manos de personas no autorizadas, es decir, que ni tienen la habilitación de seguridad ni la necesidad de conocer pertinentes, o cuando existe la probabilidad de que se haya producido este hecho.

La información clasificada de la UE puede exponerse a riesgo por descuido, negligencia o indiscreción, así como por las actividades de servicios de espionaje cuyo objetivo es la UE o sus Estados miembros, en lo tocante a la información clasificada y a las actividades de la UE, o por la actuación de organizaciones de carácter subversivo.

24.2. **Notificación de las infracciones de la seguridad**

Todas las personas que deban tratar información clasificada de la UE deberán recibir instrucciones detalladas sobre sus atribuciones en este ámbito. Asimismo, deberán notificar inmediatamente cualquier infracción de la seguridad de la que puedan tener conocimiento.

Cuando un responsable local de seguridad o un agente de seguridad de reunión descubra o sea informado de una infracción de la seguridad relativa a información clasificada de la UE o de la desaparición de material clasificado de la UE, deberá tomar las medidas oportunas para:

a) proteger las pruebas;

b) aclarar los hechos;

c) evaluar los daños causados y reducirlos al mínimo;

d) impedir que los hechos se repitan;

e) notificar a las autoridades competentes los efectos de la infracción de la seguridad.

En este contexto, deberán aportarse los datos siguientes:

i) descripción de la información de que se trata, con su clasificación, números de referencia y de copia, fecha, autor, asunto y ámbito;

ii) breve descripción de las circunstancias en que se ha producido la infracción de la seguridad, con la fecha y el período en que pudo exponerse a riesgo la información;

iii) declaración sobre si se ha informado al autor.

Tan pronto como se notifique que puede haberse producido una infracción, cada autoridad de seguridad deberá ponerlo inmediatamente en conocimiento de la Oficina de Seguridad de la Comisión.

Sólo se deberán notificar los casos relativos a información clasificada EU RESTRICTED cuando presenten características anómalas.

Cuando se le comunique que se ha producido una infracción de la seguridad, el miembro de la Comisión encargado de la seguridad:

a) lo notificará al autor de la información clasificada de que se trate;

b) pedirá a las autoridades de seguridad competentes que inicien una investigación;

c) coordinará las investigaciones cuando intervengan en ellas más de una instancia de seguridad;

d) obtendrá un informe sobre las circunstancias en que se produjo la infracción, la fecha o período en que pudo ocurrir y en que fue descubierta, con una descripción detallada del contenido y de la clasificación del material en cuestión; también deberá comunicarse el perjuicio ocasionado a los intereses de la UE o de alguno de sus Estados miembros, así como las medidas adoptadas para que no vuelva a suceder.

El autor deberá informar a los destinatarios y dar las instrucciones pertinentes.

24.3. **Acciones legales**

Todo individuo que sea responsable de poner en peligro información clasificada de la UE estará sujeto a medidas disciplinarias de conformidad con la normativa pertinente, en particular el título VI del Estatuto de los funcionarios. Dichas medidas no serán obstáculo para emprender otras acciones legales.

Cuando proceda y sobre la base del informe mencionado en la sección 24.2, el miembro de la Comisión encargado de la seguridad tomará todas las medidas necesarias para permitir que las autoridades nacionales competentes inicien procedimientos penales.

25. PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA DE LA UE TRATADA EN LOS SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN Y DE COMUNICACIÓN

25.1. **Introducción**

25.1.1. *Aspectos generales*

La política y los requisitos de seguridad se aplicarán a todos los sistemas y redes de comunicación (en lo sucesivo, sistemas) que traten información clasificada EU CONFIDENTIAL o de nivel superior. Se aplicarán como complemento de las disposiciones incluidas en la Decisión C(95) 1510 final de la Comisión, de 23 de noviembre de 1995, relativa la protección de los sistemas informáticos.

Los sistemas que traten información EU RESTRICTED también requerirán medidas de seguridad para proteger la confidencialidad de esa información. Todos los sistemas requerirán medidas de seguridad para proteger tanto su propia integridad y disponibilidad como la de la información que contienen.

La política de seguridad en materia de tecnología de la información aplicada por la Comisión incluye los elementos siguientes:

— constituye una parte esencial de la seguridad en general, y complementa todos los elementos relativos a la seguridad de la información, seguridad del personal y seguridad física,

— reparto de responsabilidades entre los propietarios de los sistemas técnicos, los propietarios de la información clasificada de la UE almacenada o tratada en sistemas técnicos, especialistas de la seguridad informática y usuarios,

— descripción de los principios de seguridad y de las necesidades de cada sistema de tecnología de la información,

— autorización de dichos principios y necesidades por una autoridad elegida,

— consideración de las amenazas y de las vulnerabilidades concretas en el sector de la tecnología de la información.

25.1.2. *Amenazas y vulnerabilidades de los sistemas*

Se puede definir una amenaza como la posibilidad de que la seguridad se vea puesta en peligro de forma accidental o deliberada. En el caso de los sistemas, dicha amenaza supone la pérdida de cuando menos una de las características de confidencialidad, integridad y disponibilidad. Por vulnerabilidad se entiende una debilidad o falta de control que facilitaría o permitiría el que un bien o un objetivo específicos se vieran amenazados.

La información clasificada y desclasificada de la UE tratada en los sistemas de forma concentrada para una localización, comunicación y utilización rápidas es vulnerable a numerosas amenazas. Entre ellas está el acceso de usuarios no autorizados a la información o, al contrario, la denegación del acceso a la misma a los usuarios autorizados. También hay riesgos de divulgación, corrupción, alteración o supresión no autorizadas de la información. Además, el material, complejo y a menudo frágil, resulta costoso y suele ser difícil de reparar o de sustituir rápidamente.

25.1.3. *Principal objetivo de las medidas de seguridad*

El principal objetivo de las medidas de seguridad expuestas en esta sección es prestar protección frente a la divulgación no autorizada de información clasificada de la UE (la pérdida de confidencialidad) y frente a la pérdida de integridad o de disponibilidad de la información. Para alcanzar un nivel adecuado de protección de la seguridad de un sistema que trate información clasificada de la UE, la Oficina de Seguridad de la Comisión deberá definir unas normas adecuadas de seguridad convencional junto con los procedimientos y las técnicas especiales de seguridad pertinentes particularmente ideadas para cada sistema.

25.1.4. *Enunciación de los requisitos específicos de seguridad del sistema (SSRS)*

El propietario de los sistemas técnicos (véase la sección 25.3.4) y el propietario de la información (véase la sección 25.3.5) deberán enunciar los requisitos específicos de seguridad del sistema (SSRS) para todos los sistemas que traten información clasificada EU CONFIDENTIAL o de nivel superior, con la contribución y la asistencia del personal del proyecto y de la Oficina de Seguridad de la Comisión (en calidad de Autoridad INFOSEC, véase la sección 25.3.3) y deberán ser aprobados por la Autoridad de acreditación en materia de seguridad (véase la sección 25.3.2).

Será igualmente necesario enunciar los requisitos específicos de seguridad del sistema siempre que la Autoridad de acreditación en materia de seguridad considere de capital importancia la disponibilidad e integridad de la información clasificada EU RESTRICTED o de información no clasificada.

Los requisitos específicos de seguridad del sistema deberán especificarse desde el primer momento de concepción del proyecto y deberán mejorarse y perfeccionarse a medida que el proyecto avance, de forma que desempeñen diversas funciones en las diferentes fases del ciclo vital del proyecto y del sistema.

25.1.5. *Modos operativos de seguridad*

Todos los sistemas que traten información clasificada EU CONFIDENTIAL o de nivel superior estarán autorizados para funcionar en uno de los siguientes modos de operación de seguridad o en su equivalente nacional o, cuando fuere necesario y por períodos diferentes, en más de uno de los siguientes modos de operación de seguridad:

a) exclusivo;

b) de alto nivel;

c) de múltiples niveles.

25.2. **Definiciones**

Por «acreditación» se entenderá la autorización y la aprobación concedidas a un sistema para tratar información clasificada de la UE en su entorno operativo.

Nota:

Dicha acreditación debe efectuarse previa aplicación de todos los procedimientos de seguridad pertinentes y de la obtención de un nivel de protección suficiente para los elementos del sistema. Normalmente, debe basarse en los requisitos específicos de seguridad del sistema y, concretamente, en los siguientes elementos:

a) una declaración del objetivo de acreditación del sistema; en particular, el nivel o niveles de clasificación de la información que deberá tratarse y el modo o modos de operación de seguridad que se proponen;

b) la elaboración de un examen de gestión de riesgos para determinar las amenazas y vulnerabilidades, así como las medidas necesarias para contrarrestarlas;

c) los procedimientos operativos de seguridad, con una descripción detallada de las operaciones propuestas (por ejemplo, modos y servicios que deberán prestarse), con una descripción de las medidas de seguridad del sistema que servirán de base a la acreditación;

d) el plan de aplicación y mantenimiento de los dispositivos de seguridad;

e) el plan que prevea las pruebas, la evaluación y la certificación tendentes a garantizar la seguridad inicial y posterior del sistema o de la red, y

f) la certificación, en su caso, junto con otros elementos de acreditación.

Por «responsable central de seguridad informática» (CISO) se entenderá el funcionario que, en un servicio central de tecnología de la información, coordina y supervisa las medidas de seguridad de los sistemas organizados de forma centralizada.

Por «certificación» se entenderá la expedición de una declaración oficial, basada en un examen independiente acerca del proceder y de los resultados de una evaluación, que indique en qué medida un sistema cumple la exigencia de seguridad o un producto de seguridad informática cumple los requisitos de seguridad previamente establecidos.

Por «seguridad de las comunicaciones» (COMSEC) se entenderá la aplicación a las telecomunicaciones de medidas de seguridad encaminadas a denegar a las personas no autorizadas información útil que pudiera derivarse de la posesión y el estudio de dichas telecomunicaciones o a garantizar la autenticidad de las mismas.

Nota:

Dichas medidas incluyen tanto la seguridad en materia de criptografía, transmisión y emisión como la seguridad relativa a los procedimientos, a los elementos físicos, al personal, a los documentos y al ordenador.

Por «seguridad de los ordenadores» (COMPUSEC) se entenderá la aplicación a un sistema informático de dispositivos de seguridad del soporte material, de los microprogramas y de los programas informáticos con objeto de protegerle contra, o impedir, la divulgación, manipulación, modificación o supresión de información no autorizadas, o la denegación de servicio.

Por «producto de seguridad informática» se entenderá un elemento genérico de seguridad informática destinado a ser incorporado a un sistema de tecnología de la información con objeto de mejorar o garantizar la confidencialidad, la integridad o la disponibilidad de la información tratada.

Por «modo de operación de seguridad exclusivo» se entenderá un modo de operación en el que TODOS los individuos con acceso al sistema están habilitados al nivel más alto de clasificación de la información tratada en el sistema, y con una necesidad común de conocer TODA la información tratada en el sistema.

Notas:

(1) La necesidad común de conocer indica que no existe un requisito obligatorio de que los dispositivos de seguridad informática permitan separar la información dentro del sistema.

(2) Otros dispositivos de seguridad (por ejemplo, físicos, administrativos y de procedimiento) deberán ajustarse a los requisitos del nivel más alto de clasificación y de todas las designaciones de las diversas categorías de información tratada en el sistema.

Por «evaluación» se entenderá el examen técnico detallado, por una autoridad pertinente, de los aspectos de seguridad de un sistema o de un producto para la seguridad de la criptografía o del ordenador.

Notas:

(1) La evaluación investiga la presencia de la funcionalidad de seguridad requerida y la ausencia de efectos secundarios indeseables que se deriven de dicha funcionalidad; asimismo, valora la inalterabilidad de esa funcionalidad.

(2) La evaluación determina la medida en que se cumplen los requisitos de seguridad de un sistema o las exigencias de seguridad de un producto de seguridad informática, y establece el nivel de garantía del sistema o de la función de confianza del producto de seguridad informática.

Por «propietario de la información» (IO) se entenderá la autoridad (Jefe de Unidad) que tiene la responsabilidad de crear, procesar y utilizar la información, incluida la capacidad de decidir quién está autorizado a acceder a dicha información.

Por «seguridad de la información» (INFOSEC) se entenderá la aplicación de medidas de seguridad para proteger la información tratada, almacenada o transmitida en sistemas electrónicos de comunicación, información u otros, frente a una pérdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, y para evitar la pérdida de integridad y disponibilidad de los sistemas en sí mismos.

Las «medidas de INFOSEC» incluyen la seguridad de los ordenadores, de las transmisiones, de las emisiones y la seguridad de carácter criptográfico, así como la detección, documentación y respuesta a las amenazas contra la información y los sistemas.

Por «zona de tecnología de la información» se entenderá una zona que contiene uno o varios ordenadores, sus unidades locales periféricas y de archivo, la unidad de control, las redes exclusivas y el equipo de comunicaciones.

Nota:

Esto no incluye una zona aparte donde haya terminales, puestos de trabajo o periféricos remotos, aun cuando dichos dispositivos estén conectados al equipo que se encuentra en la zona de tecnología de la información.

Por «red de tecnología de la información» se entenderá la organización, geográficamente dispersa, de sistemas de tecnología de la información interconectados para el intercambio de datos, incluidos los componentes de los sistemas de tecnología de la información interconectados y su interfaz con las redes de datos o redes de comunicación de apoyo.

Notas:

(1) Una red de tecnología de la información puede utilizar los servicios de una o varias redes de comunicación interconectadas para el intercambio de datos; varias redes de tecnología de la información pueden utilizar los servicios de una red común de comunicación.

(2) Una red de tecnología de la información se denomina «local» si conecta varios ordenadores que se encuentren en el mismo lugar.

Los «dispositivos de seguridad de una red de tecnología de la información» comprenden los dispositivos de seguridad de cada sistema de tecnología de la información que forme parte de la red, pero también los componentes y dispositivos complementarios asociados a dicha red y necesarios para garantizar un nivel aceptable de protección de la información clasificada (por ejemplo, comunicaciones en red, mecanismos y procedimientos de etiquetado e identificación de seguridad, controles de acceso, programas y ficheros de seguimiento).

Por «sistema de tecnología de la información» se entenderá un conjunto de material, métodos, procedimientos y, si es necesario, personal, organizado de forma que cumpla funciones de tratamiento de la información.

Notas:

(1) Se trata de un conjunto de estructuras configuradas para tratar información dentro del sistema.

(2) Dichos sistemas pueden servir de apoyo a la consulta, comando, control y comunicación, así como a aplicaciones científicas o administrativas, incluido el tratamiento de textos.

(3) Los límites de un sistema se determinarán generalmente como los elementos que están bajo el control de un único propietario de los sistemas técnicos.

(4) Un sistema de tecnología de la información podrá contener subsistemas, algunos de los cuales serán sistemas de tecnología de la información en sí mismos.

Las «medidas de seguridad de un sistema de tecnología de la información» comprenden todas las funciones y características de soporte material, microprogramas y programas informáticos; procedimientos operativos, procedimientos de responsabilidad y controles de acceso, zona de tecnología de la información, zona de terminales o puestos de trabajo remotos, así como las normas de gestión, los dispositivos y estructuras físicas, las medidas de control de personal y de las comunicaciones necesarias para garantizar un nivel aceptable de protección de la información clasificada que deberá tratarse en un sistema de tecnología de la información.

Por «responsable local de seguridad informática» (LISO) se entenderá el funcionario que, en un servicio de la Comisión, se encarga de coordinar y supervisar las medidas de seguridad dentro de su ámbito de actuación.

Por «modo de operación de seguridad de múltiples niveles» se entenderá un modo de operación en el que NO TODOS los individuos con acceso al sistema están habilitados al nivel más alto de clasificación de la información tratada en el sistema, y en el cual NO TODOS los individuos con acceso al sistema tienen una necesidad común de conocer la información tratada en el sistema.

Notas:

(1) Este modo de operación permite, simultáneamente, el tratamiento de informaciones de diversos niveles de clasificación y de diferentes designaciones de categoría de información.

(2) El hecho de que no todos los individuos estén habilitados al nivel más alto y no tengan una necesidad común de conocer indica que existe el requisito de que las medidas de seguridad informática permitan un acceso selectivo a la información presente en el sistema y la separación de dicha información dentro del sistema.

Por «zona de terminales o puestos de trabajo remotos» se entenderá una zona que contiene equipo informático, sus periféricos, terminales o puestos de trabajo locales y cualquier equipo de comunicaciones asociado, separada de una zona de tecnología de la información.

Por «procedimientos operativos de seguridad» se entenderá los procedimientos elaborados por el propietario de los sistemas técnicos para definir los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal.

Por «modo de operación de seguridad de alto nivel» se entenderá un modo de operación en el que TODOS los individuos con acceso al sistema están habilitados al nivel más alto de clasificación de la información tratada en el sistema, pero en el que NO TODOS los individuos con acceso al sistema tienen una necesidad común de conocer la información tratada en el sistema.

Notas:

(1) La falta de una necesidad común de conocer indica la existencia del requisito de que los dispositivos de seguridad informática permitan un acceso selectivo a la información presente en el sistema y la separación de dicha información dentro del sistema.

(2) Otros dispositivos de seguridad (por ejemplo, físicos, de personal y de procedimiento) deberán ajustarse a los requisitos del nivel más alto de clasificación y de todas las designaciones de las diversas categorías de información tratada en el sistema.

(3) Todas las informaciones tratadas o disponibles de un sistema en este modo de operación, al igual que el producto generado, estarán protegidas al nivel potencialmente más alto de la designación de la categoría y al nivel más alto de la clasificación de la información tratada hasta que se decida lo contrario, a menos que exista una función de etiquetado suficientemente fiable.

Por «enunciación de los requisitos específicos de seguridad del sistema» (SSRS) se entenderá una enumeración completa y explícita de los principios de seguridad que deben observarse y de los requisitos pormenorizados de seguridad que hay que cumplir. Se basan en la política de seguridad y de evaluación de riesgos de la Comisión, o vienen impuestos por parámetros como el entorno operativo, el nivel más bajo de habilitación de seguridad del personal, la clasificación más alta de la información tratada, el modo operativo de seguridad o las necesidades de los usuarios. Los requisitos específicos de seguridad del sistema forman parte integrante de la documentación del proyecto presentada a las autoridades competentes para su aprobación técnica, presupuestaria y de seguridad. En su forma final, los requisitos específicos de seguridad del sistema constituyen una verdadera enumeración de los parámetros de seguridad del sistema.

Por «propietario de los sistemas técnicos» (TSO) se entenderá la autoridad responsable de la creación, mantenimiento, explotación y cierre de un sistema.

Por «contramedidas TEMPEST» se entenderá las medidas de seguridad destinadas a proteger el equipo y las infraestructuras de comunicación frente al riesgo de que se filtre información clasificada a través de emisiones electromagnéticas no intencionadas.

25.3. **Competencias en materia de seguridad**

25.3.1. *Aspectos generales*

Las competencias consultivas del Grupo consultivo sobre la política de seguridad de la Comisión, definidas en la sección 12, incluyen cuestiones INFOSEC. Este grupo organizará sus actividades de tal manera que pueda facilitar un asesoramiento experto en las cuestiones antes mencionadas.

La Oficina de Seguridad de la Comisión será la encargada de publicar normas INFOSEC detalladas, a partir de las disposiciones del presente capítulo.

En caso de que surjan problemas relativos a la seguridad (incidentes, quebrantamientos, etc.), la Oficina de Seguridad de la Comisión deberá adoptar medidas inmediatas.

La Oficina de Seguridad de la Comisión dispondrá de una unidad INFOSEC.

25.3.2. *La Autoridad de acreditación en materia de seguridad (SAA)*

El jefe de la Oficina de Seguridad de la Comisión será la Autoridad de acreditación en materia de seguridad de la Comisión. La Autoridad de acreditación en materia de seguridad será responsable de la organización general de la seguridad y de los ámbitos INFOSEC especializados, a saber, la seguridad de las comunicaciones, la seguridad Crypto y la seguridad Tempest.

La Autoridad de acreditación en materia de seguridad se encargará de garantizar la conformidad de los sistemas con la política de seguridad de la Comisión. Una de sus tareas consistirá en otorgar la aprobación de un sistema para tratar información clasificada de la UE a un nivel de clasificación definido en su entorno operativo.

La jurisdicción de la SAA de la Comisión incluirá todos los sistemas operativos en los locales de la Comisión. Cuando diversos componentes de un sistema recaigan en la jurisdicción de la SAA de la Comisión y de otras SAA, todas las partes en cuestión podrán designar un comité común de acreditación bajo la coordinación de la SAA de la Comisión.

25.3.3. *La Autoridad INFOSEC (IA)*

El jefe de la Unidad INFOSEC de la Oficina de Seguridad de la Comisión será la Autoridad INFOSEC de la Comisión. La Autoridad INFOSEC se encargará de las siguientes actividades:

— facilitar asesoramiento técnico y asistencia a la Autoridad de acreditación en materia de seguridad,

— prestar asistencia en el desarrollo de los requisitos específicos de seguridad del sistema,

— revisar los requisitos específicos de seguridad del sistema para garantizar su coherencia con las presentes normas de seguridad y con los documentos relativos a la política y la arquitectura INFOSEC,

— participar en los grupos o comités de acreditación, cuando sea necesario, así como facilitar a la Autoridad de acreditación en materia de seguridad recomendaciones INFOSEC sobre la acreditación,

— facilitar apoyo a las actividades de formación e información INFOSEC,

— facilitar asesoramiento técnico en las investigaciones sobre incidentes relacionados con INFOSEC,

— definir directrices técnico-políticas para garantizar que únicamente se utilicen programas informáticos autorizados.

25.3.4. *El propietario de los sistemas técnicos*

La responsabilidad de la ejecución y del funcionamiento de los controles y de los dispositivos de seguridad especiales de un sistema recae en el propietario de dicho sistema, el propietario de los sistemas técnicos. En el caso de los sistemas gestionados a escala central, deberá nombrarse un responsable central de seguridad informática. Cada servicio nombrará, según proceda, un responsable local de seguridad informática. La responsabilidad de un propietario de los sistemas técnicos incluye la elaboración de procedimientos operativos de seguridad y se prolongará durante el ciclo vital de un sistema, desde la fase de concepción del proyecto hasta su descarte definitivo.

El propietario de los sistemas técnicos especificará las normas y prácticas de seguridad que deba cumplir el suministrador del sistema.

El propietario de los sistemas técnicos podrá delegar una parte de sus responsabilidades, por ejemplo, en el responsable local de seguridad informática. Una sola persona podrá realizar las diversas funciones de INFOSEC.

25.3.5. *El propietario de la información (IO)*

El propietario de la información será responsable de la información clasificada de la UE (y de otro tipo de información) que deba ser introducida, procesada y producida en los sistemas técnicos. Definirá las exigencias para el acceso a dicha información en los sistemas. Podrá delegar su responsabilidad en un gestor de la información o en un gestor de base de datos dentro de su ámbito de actuación.

25.3.6. *Usuarios*

Todos los usuarios serán responsables de garantizar que sus acciones no pongan en peligro la seguridad del sistema que utilizan.

25.3.7. *Formación INFOSEC*

Se ofrecerá formación e información INFOSEC a todo el personal que lo necesite.

25.4. **Medidas de seguridad de carácter no técnico**

25.4.1. *Seguridad de personal*

Los usuarios del sistema deberán estar habilitados y tener necesidad de conocer, según corresponda a la clasificación y al contenido de la información tratada en su sistema específico. El acceso a determinadas informaciones o equipos específicos de sistemas de seguridad requerirá una autorización especial otorgada con arreglo a los procedimientos de la Comisión.

La Autoridad de acreditación en materia de seguridad designará todos los puestos sensibles y definirá el nivel de autorización y supervisión exigido a todo el personal que los ocupe.

Los sistemas deberán especificarse y concebirse de forma que se facilite la distribución de tareas y responsabilidades entre el personal para que ninguna persona tenga el conocimiento ni el control completo de los puntos clave de seguridad del sistema.

Las zonas de tecnología de la información y las zonas de terminales o puestos de trabajo remotos donde la seguridad del sistema pueda alterarse no estarán ocupadas por un solo funcionario u otro agente autorizado.

Las normas de seguridad de un sistema sólo podrán ser modificadas por al menos dos personas autorizadas que actúen de común acuerdo.

25.4.2. *Seguridad física*

Las zonas de tecnología de la información y las zonas de terminales o puestos de trabajo remotos (según la definición que consta en la sección 25.2) en las que una información clasificada EU CONFIDENTIAL y de nivel superior se trate con medios de tecnología de la información, o en las cuales sea posible un acceso a tal información, se clasificarán como zonas de seguridad de la UE de clase I o clase II, según convenga.

25.4.3. *Control de acceso a un sistema*

Toda la información y todo el material que controlen el acceso a un sistema estarán protegidos según las disposiciones correspondientes a la clasificación más alta y a la categoría de información a la cual dicho sistema pueda dar acceso.

Cuando ya no se utilice para dicho fin, la información y el material de control de acceso deberán ser destruidos de conformidad con las disposiciones de la sección 25.5.4.

25.5. **Medidas de seguridad de carácter técnico**

25.5.1. *Seguridad de la información*

El autor de la información tendrá la obligación de identificar y clasificar todos los documentos que contengan información ya sea en forma de impresión en papel o de soporte informático. En cada página del producto impreso se indicará, tanto en la cabecera como al pie, la clasificación correspondiente. Los documentos producidos, ya sean en forma de impresión en papel o de soporte informático, tendrán la misma clasificación que la información de nivel más alto que se haya utilizado para producirlos. El modo en que se opere un sistema podrá también repercutir en la clasificación de los documentos producidos por ese sistema.

Los servicios de la Comisión y quienes detenten en ella una información estarán obligados a considerar los problemas que plantean la suma de elementos discretos de información y las deducciones que puedan hacerse de los elementos interrelacionados, así como a determinar si es pertinente una clasificación de nivel más alto para la totalidad de la información.

El hecho de que la información pueda representarse en forma de código abreviado, de código de transmisión, o en cualquier otra forma binaria, no le garantiza protección alguna y, por tanto, no deberá incidir en la clasificación de la información.

Cuando la información se transfiera de un sistema a otro, deberá protegerse durante el traslado y en el sistema receptor de manera conforme a la clasificación y a la categoría originales de la información.

Todos los soportes informáticos deberán tratarse de conformidad con la clasificación más alta de la información almacenada o de su marcado, y deberán estar adecuadamente protegidos en todo momento.

Los soportes informáticos reutilizables que sirvan para registrar información clasificada de la UE mantendrán el nivel más alto de clasificación atribuido a los datos para los que hayan sido utilizados hasta que dicha información se recalifique o desclasifique y el soporte se vuelva a clasificar de manera correspondiente, o se desclasifique o destruya de conformidad con un procedimiento aprobado por la Autoridad de acreditación en materia de seguridad (véase 25.5.4).

25.5.2. *Control y responsabilización de la información*

Deberán llevarse registros automáticos (inspecciones de seguimiento) o manuales para dejar constancia del acceso a la información clasificada EU SECRET y de nivel superior. Dichos registros se conservarán de conformidad con las presentes normas de seguridad.

Los productos clasificados de la UE que se mantengan en la zona de tecnología de la información podrán tratarse como un único elemento clasificado y no hará falta que se registren, siempre y cuando el material sea identificado, lleve marcada su clasificación y esté debidamente controlado.

Cuando un sistema genere un producto que trate información clasificada de la UE y se transmita de una zona de tecnología de la información a una zona de terminales o puestos de trabajo remotos, se crearán procedimientos, aprobados por la Autoridad de acreditación en materia de seguridad, para controlar y registrar dicho producto. Para la clasificación EU SECRET y de nivel superior, dichos procedimientos incluirán instrucciones específicas respecto de la fiabilidad de la información.

25.5.3. *Tratamiento y control de los soportes informáticos extraíbles*

Todos los soportes informáticos extraíbles clasificados EU CONFIDENTIAL y de nivel superior se tratarán como material clasificado y se les aplicarán las normas generales. Será preciso adaptar la correspondiente identificación y clasificación a las características físicas de los soportes, con objeto de que puedan reconocerse con toda claridad.

Incumbirá a los usuarios garantizar que la información clasificada de la UE se archive en soportes que tengan la indicación de clasificación y la protección adecuadas. Se establecerán procedimientos para garantizar que, a todos los niveles de información de la UE, el archivo de la información en soportes informáticos tenga lugar de conformidad con las presentes normas de seguridad.

25.5.4. *Desclasificación y destrucción de soportes informáticos*

Los soportes informáticos utilizados para registrar información clasificada de la UE podrán ser recalificados o desclasificados de conformidad con un procedimiento aprobado por la Autoridad de acreditación en materia de seguridad.

Los soportes informáticos que hayan contenido información clasificada EU TOP SECRET o información de categoría especial no serán desclasificados ni reutilizados.

Los soportes informáticos que no puedan desclasificarse ni reutilizarse se destruirán de conformidad con el procedimiento anteriormente mencionado.

25.5.5. *Seguridad de las comunicaciones*

El jefe de la Oficina de Seguridad de la Comisión será la Autoridad Crypto.

Cuando una información clasificada de la UE se transmita por vía electromagnética, se aplicarán medidas especiales para proteger la confidencialidad, integridad y disponibilidad de dicha transmisión. La Autoridad de acreditación en materia de seguridad determinará los requisitos relativos a la protección de las transmisiones frente a la detección y la interceptación. La información transmitida dentro de un sistema de comunicaciones estará protegida conforme a los requisitos de confidencialidad, integridad y disponibilidad.

Cuando sea preciso recurrir a métodos criptográficos para proteger la confidencialidad, integridad y disponibilidad, dichos métodos y sus productos asociados deberán ser expresamente aprobados a tal fin por la Autoridad de acreditación en materia de seguridad en calidad de Autoridad Crypto.

Durante la transmisión, la confidencialidad de la información clasificada EU SECRET o de nivel superior estará protegida por métodos o productos criptográficos aprobados por el miembro de la Comisión encargado de la seguridad previa consulta al Grupo consultivo sobre la política de seguridad de la Comisión. Durante la transmisión, la confidencialidad de la información clasificada EU CONFIDENTIAL o EU RESTRICTED estará protegida por métodos o productos criptográficos aprobados por la Autoridad Crypto de la Comisión previa consulta al Grupo consultivo sobre la política de seguridad de la Comisión.

Se establecerán normas detalladas aplicables a la transmisión de información clasificada de la UE en las instrucciones específicas de seguridad aprobadas por la Oficina de Seguridad de la Comisión previa consulta al Grupo consultivo sobre la política de seguridad de la Comisión.

En circunstancias operativas excepcionales, la información clasificada EU RESTRICTED, EU CONFIDENTIAL y EU SECRET podrá transmitirse en forma de texto claro siempre y cuando el propietario de la información lo autorice expresamente en cada ocasión y lo registre debidamente. Dichas circunstancias excepcionales son las siguientes:

a) en circunstancias, inminentes o en curso, de crisis, conflictos o guerras; y

b) cuando la rapidez de la transmisión sea de la mayor importancia, no se disponga de medios de cifrado y se considere que la información transmitida no puede explotarse en un lapso de tiempo que influya negativamente en las operaciones.

Un sistema deberá tener la capacidad de denegar de forma concluyente el acceso a información clasificada de la UE a cualquiera de sus terminales o puestos de trabajo remotos, si es necesario desconectándolos físicamente o mediante dispositivos informáticos especiales aprobados por la Autoridad de acreditación en materia de seguridad.

25.5.6. *Seguridad en materia de instalación y radiaciones*

En las especificaciones de la instalación inicial de los sistemas y de cualquier modificación posterior de la misma deberá establecerse que éstas se efectúan por instaladores provistos de la necesaria autorización de seguridad, bajo la vigilancia continua de un personal técnico competente habilitado para tener acceso a información clasificada de la UE de un nivel de clasificación equivalente a la clasificación más alta que el sistema deba almacenar y tratar.

Los sistemas que traten información clasificada EU CONFIDENTIAL o de nivel superior estarán protegidos de tal modo que su seguridad no pueda estar amenazada por radiaciones o una conductividad perjudiciales, cuyo examen y prevención se designarán con el término «Tempest».

Las contramedidas Tempest serán estudiadas y aprobadas por una autoridad Tempest (véase 25.3.2).

25.6. **Seguridad durante el tratamiento**

25.6.1. *Procedimientos operativos de seguridad (SecOPS)*

Los procedimientos operativos de seguridad definen los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal y se elaborarán bajo la responsabilidad del propietario de los sistemas técnicos.

25.6.2. *Gestión de la protección y configuración de los programas informáticos*

La protección de seguridad de los programas de aplicación se determinará a tenor de una evaluación de la clasificación de seguridad del propio programa y no de la clasificación de la información que deban tratar. Las versiones de los programas informáticos utilizados deberán comprobarse periódicamente para garantizar su integridad y correcto funcionamiento.

No se utilizarán versiones nuevas o modificadas de los programas informáticos para el tratamiento de la información clasificada de la UE hasta que el propietario de los sistemas técnicos los haya comprobado.

25.6.3. *Control de la presencia de virus y programas informáticos destinados a causar daños*

Se llevarán a cabo controles para detectar la presencia de virus y programas informáticos destinados a causar daños, de conformidad con los requisitos de la Autoridad de acreditación en materia de seguridad.

Antes de su integración en cualquier sistema, todos los soportes informáticos que lleguen a la Comisión deberán verificarse con objeto de detectar la presencia de cualquier virus o programa informático destinado a causar daños.

25.6.4. *Mantenimiento*

Los contratos y procedimientos para el mantenimiento, ya sea éste programado o realizado previa petición, de los sistemas para los que se haya efectuado unos requisitos específicos de seguridad del sistema especificarán los requisitos y las disposiciones aplicables al personal de mantenimiento y al equipo correspondiente que entre en una zona de tecnología de la información.

Los requisitos y procedimientos se indicarán con claridad, respectivamente, en los requisitos específicos de seguridad del sistema y en los procedimientos operativos de seguridad. Las instrucciones de mantenimiento del contratista que requieran procedimientos de diagnóstico de acceso remoto se permitirán únicamente en circunstancias excepcionales, bajo un riguroso control de seguridad y sólo con la aprobación de la Autoridad de acreditación en materia de seguridad.

25.7. **Adquisición**

25.7.1. *Aspectos generales*

Todo producto de seguridad que vaya a utilizarse con el sistema que va a adquirirse deberá haber sido evaluado y certificado o ser objeto de evaluación y certificación en el momento de la adquisición por parte de un organismo de evaluación o certificación adecuado de uno de los Estados miembros según criterios reconocidos a escala internacional (tales como los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, véase norma ISO 15408). Para obtener la autorización de la Comisión Consultiva de Compras y Contratos (CCCC) se exigen procedimientos específicos.

Al decidir si el equipo y, en particular, los soportes informáticos deben arrendarse en vez de adquirirse, deberá tenerse presente que dicho equipo, una vez utilizado para tratar información clasificada de la UE, no podrá utilizarse fuera de un entorno adecuadamente seguro sin ser primero desclasificado con la aprobación de la Autoridad de acreditación en materia de seguridad, y que dicha aprobación no siempre será posible.

25.7.2. *Acreditación*

Antes de tratar información clasificada de la UE, todos los sistemas para los que se necesite unos requisitos específicos de seguridad del sistema deberán ser acreditados por la Autoridad de acreditación en materia de seguridad a tenor de la información contenida en los requisitos específicos de seguridad del sistema, en los procedimientos operativos de seguridad y en cualquier otro documento aplicable. Los subsistemas y los terminales y puestos de trabajo remotos deberán estar acreditados como parte de todos los sistemas a los que estén conectados. Cuando un sistema sirva al mismo tiempo a la Comisión y a otras organizaciones, la Comisión y las autoridades de seguridad pertinentes acordarán mutuamente la acreditación.

El proceso de acreditación podrá efectuarse con arreglo a una estrategia de acreditación adecuada a un determinado sistema y definida por la Autoridad de acreditación en materia de seguridad.

25.7.3. *Evaluación y certificación*

En determinados casos, antes de su acreditación, el soporte material, los microprogramas y los dispositivos de seguridad informáticos de un sistema se evaluarán y certificarán como capaces de salvaguardar información en el nivel de clasificación pertinente.

Los requisitos para la evaluación y certificación se incluirán en la planificación del sistema y se indicarán claramente en los requisitos específicos de seguridad del sistema.

Los procesos de evaluación y certificación se llevarán a cabo de conformidad con las directrices aprobadas por personal técnicamente cualificado y debidamente habilitado que actúe en nombre del propietario de los sistemas técnicos.

El personal podrá ser el indicado por una autoridad nacional de evaluación o certificación designada o por sus representantes designados, por ejemplo un contratista competente y habilitado.

El grado de los procesos de evaluación y certificación necesarios podrá reducirse (por ejemplo, para incluir únicamente los aspectos de integración) cuando los sistemas se basen en productos para la seguridad informática evaluados y certificados a escala nacional.

25.7.4. *Control sistemático de los elementos de seguridad para una acreditación continua*

El propietario de los sistemas técnicos deberá establecer procedimientos de control sistemático que garanticen que todos los dispositivos de seguridad del sistema siguen siendo válidos.

Los tipos de modificación que requieran una nueva acreditación o la aprobación previa de la Autoridad de acreditación en materia de seguridad deberán identificarse claramente y enunciarse en los requisitos específicos de seguridad del sistema. Después de cualquier modificación, reparación o fallo que pueda haber afectado a los dispositivos de seguridad del sistema, el propietario de los sistemas técnicos se encargará de que se realice un control para garantizar el funcionamiento correcto de los dispositivos de seguridad. La acreditación del sistema dependerá normalmente del resultado satisfactorio de dichos controles.

La Autoridad de acreditación en materia de seguridad inspeccionará o revisará periódicamente todos los sistemas a los que se hayan aplicado dispositivos de seguridad. Con respecto a los sistemas que traten información clasificada EU TOP SECRET, las inspecciones se efectuarán al menos una vez al año.

25.8. **Utilización temporal u ocasional**

25.8.1. *Seguridad de los microordenadores y de los ordenadores personales (PC)*

Los microordenadores y ordenadores personales con disco fijo (u otros soportes de memoria permanente), que funcionen autónomamente o en red, y los dispositivos informáticos portátiles (por ejemplo, PC portátiles y «notebooks» electrónicos) con discos duros fijos, se considerarán medios de almacenamiento de información en el mismo sentido que los disquetes u otros soportes informáticos extraíbles.

Se aplicará a dichos equipos, por lo que respecta al acceso, tratamiento, almacenamiento y transporte, el nivel de protección correspondiente al nivel más alto de clasificación de la información que se haya almacenado o tratado (hasta que se recalifiquen o desclasifiquen con arreglo a procedimientos aprobados).

25.8.2. *Utilización de equipos privados para trabajos oficiales de la Comisión*

Para tratar información clasificada de la UE queda prohibida la utilización de soportes informáticos extraíbles, programas informáticos y soportes materiales de tecnología de la información privados (por ejemplo, PC y dispositivos informáticos portátiles) con capacidad de archivar datos.

No podrán introducirse soportes materiales, programas informáticos y soportes informáticos privados en una zona de clase I o clase II en que se trate información clasificada de la UE sin la autorización escrita del Jefe de la Oficina de Seguridad de la Comisión. Dicha autorización únicamente se concederá por razones técnicas en casos excepcionales.

25.8.3. *Utilización de equipo perteneciente a un contratista facilitado por un país para un trabajo oficial de la Comisión*

El jefe de la Oficina de Seguridad de la Comisión podrá autorizar la utilización de equipo de tecnología de la información y de programas informáticos pertenecientes a un contratista en organizaciones que prestan apoyo a los trabajos oficiales de la Comisión. Asimismo podrá autorizar la utilización de equipo de tecnología de la información y de programas informáticos suministrados por un país; en tal caso, el equipo de tecnología de la información se someterá al control del inventario adecuado de la Comisión. En ambos casos, si el equipo de tecnología de la información sirve para tratar información clasificada de la UE, se consultará a la Autoridad de acreditación en materia de seguridad con objeto de que se consideren y lleven a efecto debidamente los elementos de INFOSEC que sean aplicables a la utilización de ese equipo.

26. ENTREGA DE INFORMACIÓN CLASIFICADA DE LA UE A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

26.1.1. *Principios que rigen la comunicación de información clasificada de la UE*

El colegio de miembros de la Comisión decidirá comunicar la información clasificada de la UE a terceros países u organizaciones internacionales a tenor:

— del carácter y el contenido de dicha información,

— de la «necesidad de conocer» de los destinatarios,

— de la apreciación de las ventajas para la UE.

Se solicitará la aprobación del autor de la información clasificada de la UE que deba entregarse.

Dichas decisiones se adoptarán caso por caso, en función:

— del grado de cooperación deseado con los terceros países u organizaciones internacionales de que se trate,

— de la confianza que se les pueda otorgar, que se deriva del nivel de seguridad que se aplicaría a la información clasificada de la UE confiada a dichos países u organizaciones y de la coherencia entre las normas de seguridad aplicables en dichos países u organizaciones y las aplicadas en la UE; el Grupo consultivo sobre la política de seguridad de la Comisión facilitará a la Comisión su dictamen técnico sobre este punto.

La aceptación por terceros países u organizaciones internacionales de la información clasificada de la UE supondrá la garantía de que dicha información no se utilizará con fines distintos de los que han motivado la comunicación o el intercambio de información y de que dichos países u organizaciones proporcionarán la protección exigida por la Comisión.

26.1.2. *Niveles*

Una vez que la Comisión haya decidido que una información clasificada puede comunicarse o intercambiarse con un determinado país u organización internacional, decidirá sobre el nivel de cooperación que resulta posible. Ello dependerá, en particular, de la política y la normativa de seguridad que se aplique en dicho país u organización

Existen tres niveles de cooperación:

Nivel 1

Cooperación con terceros países u organizaciones internacionales cuyas política y normativa de seguridad son muy similares a las de la UE.

Nivel 2

Cooperación con terceros países u organizaciones internacionales cuyas política y normativa de seguridad son notablemente distintas de las de la UE.

Nivel 3

Cooperación ocasional con terceros países u organizaciones internacionales cuyas política y normativa de seguridad no pueden evaluarse.

Cada nivel de cooperación determinará los procedimientos y disposiciones de seguridad, expuestos en los Apéndices 3, 4 y 5.

26.1.3. *Acuerdos en materia de seguridad*

Una vez que la Comisión haya decidido que existe una necesidad permanente o a largo plazo de intercambiar información clasificada entre la Comisión y terceros países u otras organizaciones internacionales, celebrará con ellos «acuerdos sobre los procedimientos de seguridad para el intercambio de información clasificada» que definan el objeto de la cooperación y las normas de protección recíproca de la información intercambiada

En el caso de la cooperación ocasional de nivel 3 que, por definición, está limitada en el tiempo y en su objeto, podrá hacer las veces de «acuerdo sobre los procedimientos para el intercambio de información clasificada» un simple memorando de entendimiento que defina el carácter de la información clasificada que deba intercambiarse y las obligaciones recíprocas con respecto a dicha información, a condición de que dicho memorando no sea de clasificación más alta que EU RESTRICTED.

Los proyectos de acuerdo sobre procedimientos de seguridad o los memorandos de entendimiento serán debatidos por el Grupo consultivo sobre la política de seguridad de la Comisión antes de someterlos a la Comisión para que ésta decida.

El miembro de la Comisión encargado de los temas de seguridad solicitará toda la asistencia necesaria de la Autoridad de seguridad nacional de los Estados miembros para garantizar que la información que deba comunicarse se utilice y proteja de conformidad con lo dispuesto en los acuerdos sobre procedimientos de seguridad o memorandos de entendimiento.

Apéndice 1

COMPARACIÓN DE LAS CLASIFICACIONES DE SEGURIDAD NACIONALES

Clasificación UE	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
Clasificación OTAN (1)				
Clasificación UEO	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Clasificación EURATOM (2)	EURATOM Top Secret	EURATOM Secret	EURATOM Confidential	EURATOM Restricted
Bélgica	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Dinamarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Alemania	STRENG GEHEIM	GEHEIM	VS (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grecia	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
España	Secreto	Reservado	Confidencial	Difusión limitada
Francia	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlanda	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburgo	Très Secret	Secret	Confidentiel	Diffusion restreinte
Países Bajos	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finlandia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Suecia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Reino Unido	Top Secret	Secret	Confidential	Restricted

(1) OTAN: La correspondencia con las categorías de clasificación de la OTAN se determinará cuando se negocie el acuerdo de seguridad entre la Comisión y la OTAN.
(2) Reglamento Euratom nº 3 de 31 de julio de 1958 sobre la protección de la información clasificada de Euratom.
(3) Alemania: VS = Verschlusssache.
(4) Francia: La clasificación «Très Secret Défense», que se refiere a asuntos prioritarios del Gobierno, sólo puede cambiarse con la autorización del Primer Ministro.

Apéndice 2

GUÍA PRÁCTICA DE CLASIFICACIÓN

Esta guía es indicativa y no debe interpretarse que modifica las disposiciones sustantivas expuestas en las secciones 16, 17, 20 y 21.

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
EU TOP SECRET: Esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros [16.1].	Se existe la probabilidad de que poner en peligro materiales clasificados EU TOP SECRET: — amenace directamente la estabilidad interna de la UE o de uno de sus Estados miembros o países amigos, — cause en perjuicio excepcionalmente grave a las relaciones con países amigos, — ponga vidas en peligro directamente, — ocasione un daño excepcionalmente grave a la capacidad de funcionar efectivamente o a la seguridad de las fuerzas de los Estados miembros o a las de otros contribuyentes, o haga que cese la efectividad de operaciones de seguridad o de inteligencia sumamente valiosas, — cause un perjuicio grave a largo plazo a los intereses económicos de la UE o de los Estados miembros.	Personas debidamente autorizadas (autores), Directores Generales, Jefes de Servicio [17.1]. Los autores deberán especificar una fecha, plazo o momento en el que el contenido pueda ser recalificado o desclasificado [16.2]. En caso contrario, revisarán los documentos en un plazo máximo de cinco años para comprobar si la clasificación original sigue siendo necesaria [17.3].	La clasificación EU TOP SECRET se aplicará a los documentos EU TOP SECRET, cuando proceda, se pondrá una indicación de seguridad y/o el marcado de protección ESDP, por medios mecánicos y a mano [16.4, 16.5, 16.3]. La clasificación de la UE y las indicaciones de seguridad aparecerán en la parte central superior y central inferior de cada página. Todas las páginas irán numeradas. Todos los documentos clasificados de la UE llevarán número de referencia y fecha. Esta referencia deberá aparecer en todas las páginas. Si se han de distribuir varias copias, cada una de ellas llevará un número de copia, que figurará en la primera página, junto con la indicación del número total de páginas. Todos los anexos y documentos adjuntos se indicarán en la primera página [21.1].	La clasificación o recalificación depende únicamente del autor, que informará de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [17.3]. Los documentos EU TOP SECRET serán distruidos por el Registo Central o registro secundario encargado de su custodia. Los documentos destruidos se relacionarán en un certificado de destrucción, firmado por el controlador EU TOP SECRET y por el funcionario que haya precensiado la destrucción que tendrá la habilitación EU TOP SECRET. En el libro de registro se hará un apunte al efecto. El registro conservará los certificados de destrucción, junto con los impresos de distribución, durante diez años [22.5].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [22.5]. Los documentos EU TOP SECRET, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos EU TOP SECRET, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos bajo la supervisión de un controlador EU TOP SECRET; la destrucción se llevará a cabo quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [22.5].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
EU SECRET: Esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros [16.1].	Si existe la probabilidad de que poner en peligro materiales clasificados EU SECRET: — cree tensiones internacionales, — cause un perjuicio grave a las relaciones con gobiernos amigos, — ponga vidas en peligro directamente o dañe gravemente el orden público o la seguridad o libertad individuales, — socasione un daño grave a la capacidad de funcionar efectivamente o a la seguridad de las fuerzas de los Estados miembros o a las de otros contribuyentes, o haga que cese la efectividad de operaciones de seguridad o de inteligencia altamente valiosas, — ocasione un considerable daño material a los intereses financieros, monetarios, económicos o comerciales de la UE o de uno de sus Estados miembros.	Personas autorizadas (autores), Directores Generales, Jefes de Servicio [17.1]. Los autores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado [16.2]. En caso contrario, se revisarán los documentos en un plazo máximo de cinco años para comprobar si la clasificación original sigue siendo necesaria [17.3].	La clasificación EU SECRET se aplicará a los documentos EU SECRET y, cuando proceda, se pondrá una indicación de seguridad y/o un marcado de protección — ESDP, por medios mecánicos y a mano [16.4, 16.5, 16.3]. Las clasificaciones de la UE y las indicaciones de seguridad aparecerán en la parte central superior y central inferior de cada página. Todas las páginas irán numeradas. Todos los documentos clasificados de la UE llevarán número de referencia y fecha; esta referencia deberá aparecer en todas las páginas. Si se han de distribuir varias copias, cada una de ellas llevará un número de copia, que figurará en la primera página, junto con la indicación del número total de páginas. Todos los anexos y documentos adjuntos se relacionarán en la primera página [21.1].	La desclasificación o recalificación depende únicamente del autor, que informará de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [17.3]. Los documentos EU SECRET serán destruidos por el registro encargado de su custodia, bajo la supervisión de una persona con habilitación de seguridad. Los documentos SECRET EU que sean destruidos se incluirán en certificados de destrucción firmados que se guardarán en el registro, junto con los impresos de destrucción, durante al menos tres años [22.5].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [22.5]. Los documentos EU SECRET, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos EU SECRET, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos; la destrucción se llevará a cabo quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [22.5].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
EU CONFIDENTIAL: Esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda suponer un perjuicio para los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros [16.1].	Si existe la probabilidad de que poner en peligro materiales clasificados EU CONFIDENTIAL: — perjudique las relaciones diplomáticas, es decir, ocasione una protesta formal u otras sanciones; — perjudique la seguridad o libertad individuales, — perjudique la capacidad de funcionar efectivamente o la seguridad de las fuerzas de los Estados miembros o las de otros contribuyentes, o disminuya la efectividad de operaciones de seguridad o de inteligencia valiosas, — menoscabe notablemente la viabilidad financiera de organizaciones importantes, — impida la investigacón de delitos graves o facilite que se cometan, — menoscabe notablemente los intereses financieros, económicos y comerciales de la UE o de sus Estados miembros, — ponga graves obstáculos al desarrollo o al funcionamiento de políticas prioritarias de la UE, — interrumpa o perturbe notablemente actividades importantes de la UE.	Personas autorizadas (autores), Directores Generales y Jefes de Servicio [17.1]. Los autores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado. En caso contrario, revisarán los documentos en un plazo máximo de cinco años, para comprobar si la clasificación original sigue siendo necesaria [17.3].	La clasificación EU CONFIDENTIAL se aplicará a los documentos EU CONFIDENTIAL, y, cuando proceda, se pondrá la indicación de seguridad y/o el marcado de protección ESDP por medios mecánicos y a mano o mediante impresión en papel preestampillado y registrado [16.4, 16.5, 16.3]. Las clasificaciones de la UE figurarán en la parte central superior y central inferior de cada página; todas las páginas irán marcadas. Todos los documentos llevarán número de referencia y fecha. Todos los anexos y documentos adjuntos se indicarán en la primera página [21.1].	La desclasificación o recalificación depende únicamente del autor, que informará de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documentos o una copia del mismo [17.3]. Los documentos EU CONFIDENTIAL serán destruidos por el registro encargado de su custodia bajo la supervisión de una persona habilitada. Se guardará constancia de su destrucción con arreglo a la normativa nacional y, en el caso de la Comisión o de los organismos descentralizados de la UE, con arreglo a las intrucciones del Presidente [22.5].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [22.5]. Los documentos EU CONFIDENTIAL, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos EU CONFIDENTIAL, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos; la destrucción, se llevará a cabo quemándolos, convertiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [22.5].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
EU RESTRICTED: Esta clasificación se aplicará a la información y al material cuya divulgación no autorizada pueda resultar desfavorable para los intereses de la Unión Europea o de uno o más de sus Estados miembros [16.1].	Si existe la probabilidad de que poner en peligro materiales clasificados EU RESTRICTED: — afecte desfavorablemente a las relaciones diplomáticas, — cause un perjuicio considerable a particulares, — dificulte el mantenimiento de la eficacia operativa o la seguridad de las fuerzas de los Estados miembros o de otros contribuyentes, — ocasione pérdidas financieras o proporcione ganancias o ventajas endebidas a particulares o empresas, — infrinja el compromiso de discreción respecto de información facilitada por terceros, — infrinja las restricciones estatutarias sobre la revelación de información, — dificulte la investigación de delitos o facilite que se cometan, — ponga en desventaja a la UE o a sus Estados miembros en negociaciones comerciales o políticas con terceros, — ponga obstáculos al desarrollo o al funcionamiento efectivos de politicas, de la UE, — menoscabe la adecuada gestión de la UE y sus operaciones.	Personas autorizadas (autores), Directores Generales, Jefes de Servicio [17.1] Los autores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado [16.2]. En caso contrario, revisarán los documentos en un plazo máximo de cinco años, con el fin de comprobar si la clasificación original sigue siendo necesaria [17.3].	La clasificación EU RESTRICTED se aplicará a los documentos EU RESTRICTED y, cuando proceda, se aplicará una indicación de seguridad y/o un marcado de protección — ESDP, por medios mecánicos o electrónicos [16.4, 16.5 y 16.3]. La clasificación de la UE y las indicaciones de seguridad figurarán en la parte superior de la primera página; todas las paginas irán numeradas. Todos los documentos clasificados de la UE llevarán número de referencia y fecha [21.1].	La desclasificación o recalificación depende únicamente del autor, que informará de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [17.3]. Los documentos EU RESTRICTED serán destruidos por el registro encargado de su custodia o por el usuario, según las intrucciones del Presidente [22.5].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [22.5].

Apéndice 3

Directrices para la entrega de información clasificada de la UE a terceros países u Organizaciones Internacionales: cooperación de nivel 1

PROCEDIMIENTO

1. Recae en el Colegio de Comisarios la autoridad para entregar información clasificada de la UE a países que no sean miembros de la Unión Europea y a organizaciones internacionales cuyas política y normativa de seguridad son comparables a las de la UE.

2. En espera de la celebración de un acuerdo de seguridad, el miembro de la Comisión encargado de la seguridad es competente para examinar las solicitudes de entrega de información clasificada de la UE.

3. Para ello, el miembro de la Comisión:
   — recabará la opinión de los autores de la información clasificada de la UE cuya entrega se solicita,
   — establecerá los contactos necesarios con los órganos de seguridad del Estado o de la organización internacional solicitante, a fin de comprobar si su política y normativa de seguridad son tales que garantizan que la información clasificada que se le entregue recibirá la protección que requieren las presentes normas de seguridad,
   — pedirá un dictamen técnico al Grupo consultivo sobre política de seguridad de la Comisión respecto de la confianza que puede depositarse en los países u organizaciones internacionales beneficiarios.

4. El miembro de la Comisión encargado de la seguridad presentará a la Comisión, para que ésta decida, la solicitud y el dictamen del Grupo consultivo sobre política de seguridad de la Comisión.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

5. El miembro de la Comisión encargado de la seguridad notificará a los países y organizaciones internacionales beneficiarios la decisión de la Comisión de autorizar la entrega de información clasificada de la UE.

6. La decisión de entregar la información no entrará en vigor hasta que los beneficiarios hayan dado garantías por escrito de que:
   — no utilizarán la información para fines distintos de los acordados,
   — protegerán la información de acuerdo con las presentes normas de seguridad y, en particular, con las disposiciones especiales que se enuncian a continuación.

7. Personal

   a) El número de funcionarios con acceso a la información clasificada de la UE estará, según el principio de necesidad de conocer, estrictamente limitado a las personas cuyas funciones hagan necesario dicho acceso.

   b) Todos los funcionarios o ciudadanos autorizados a acceder a información clasificada EU CONFIDENTIAL o de nivel superior estarán en posesión de un certificado de seguridad del nivel adecuado o de una habilitación de seguridad equivalente, cualquiera de los cuales habrá sido expedido por la administración de su país.

8. Transmisión de documentos

   a) Los procedimientos prácticos para la transmisión de documentos se decidirán por acuerdo. En espera de alcanzar dicho acuerdo se aplicarán las disposiciones de la sección 21. Dichos procedimientos especificarán, en particular, los registros a los que se remitirá la información clasificada de la UE.

   b) Si la información clasificada cuya entrega autoriza la Comisión incluye material clasificado EU TOP SECRET, el país u organización internacional beneficiario establecerá un registro central para material de la UE y, si procede, registros secundarios para ese mismo material. Estos registros se regirán por disposiciones estrictamente equivalentes a las de la sección 22 de las presentes normas de seguridad.

9. Inscripción en el registro

   No bien se reciba en un registro un documento clasificado EU CONFIDENTIAL o de nivel superior, se inscribirá el documento en un libro de registro especial que custodiará la organización. El libro de registro constará de columnas en que se indicarán la fecha de recepción, la descripción del documento (fecha, referencia y número de copia), su nivel de clasificación, su título, el nombre o cargo del receptor, la fecha del acuse de recibo y la fecha de devolución del documento al autor de la UE o de destrucción del mismo.

10. Destrucción

a) Los documentos clasificados de la UE se destruirán de conformidad con las instrucciones que figuran en la sección 22 de las presentes normas de seguridad. Se enviarán copias de los certificados de destrucción de los documentos EU SECRET y EU TOP SECRET al registro de la UE que ha transmitido los mismos.

b) Los documentos clasificados de la UE se incluirán en los planes de destrucción urgente de documentos clasificados de los organismos beneficiarios.

11. Protección de documentos

Se adoptarán todas las medidas necesarias para impedir que personas no autorizadas tengan acceso a información clasificada de la UE.

12. Copias, traducciones y extractos

No podrán hacerse fotocopias ni traducciones de los documentos clasificados EU CONFIDENTIAL o EU SECRET, ni realizarse extractos sin la autorización del jefe de la organización de seguridad de que se trate, que registrará y controlará dichas copias, traducciones o extractos y las sellará si fuera necesario.

La reproducción o la traducción de un documento EU TOP SECRET sólo podrá ser autorizada por el autor, que especificará el número de copias autorizadas. Si no puede determinarse dicho autor, la petición se remitirá a la Oficina de Seguridad de la Comisión.

13. Infracciones de la seguridad

Cuando se haya producido o se sospeche que se ha producido una infracción de la seguridad en relación con un documento clasificado de la UE, deberá actuarse inmediatamente de la siguiente forma, sin perjuicio de que se celebre un acuerdo de seguridad:

a) realizar una investigación para detectar las circunstancias de la infracción de la seguridad;

b) notificar el hecho a la Oficina de Seguridad de la Comisión, a la ANS y al autor, o, si todavía no se ha informado a este último, hacerlo constar claramente;

c) tomar medidas para reducir al mínimo los efectos de la infracción de la seguridad;

d) reconsiderar y aplicar las medidas para impedir que el hecho vuelva a suceder;

e) aplicar todas las medidas recomendadas por la Oficina de Seguridad de la Comisión para impedir que el hecho vuelva a suceder.

14. Inspecciones

Se permitirá a la Oficina de Seguridad de la Comisión, previo acuerdo con los países u organizaciones internacionales interesados, evaluar la eficacia de las medidas destinadas a proteger la información clasificada de la UE que se entregue.

15. Informe

Sin perjuicio de que se celebre un acuerdo de seguridad, mientras el país u organización internacional tenga en su poder información clasificada de la UE, deberá presentar un informe anual en la fecha que se indique cuando se conceda la autorización para entregar información. En dicho informe se confirmará que se han cumplido las presentes normas de seguridad.

Apéndice 4

Directrices para la entrega de información clasificada de la UE a terceros países u Organizaciones Internacionales: cooperación de nivel 2

PROCEDIMIENTO

1. Recae en el autor la autoridad para entregar información clasificada de la UE a terceros países u organizaciones internacionales cuyas política y normativa de seguridad son notablemente distintas de las de la UE. Recae en el Colegio de Comisarios la autoridad para entregar información clasificada de la UE originada dentro de la Comisión.

2. En principio, se limita a la información clasificada hasta el nivel EU SECRET inclusive, y no incluye la información clasificada protegida por indicaciones o marcados de seguridad especiales.

3. En espera de la celebración de un acuerdo de seguridad, el miembro de la Comisión encargado de cuestiones de seguridad es competente para examinar las solicitudes de entrega de información clasificada de la UE.

4. Para ello, el miembro de la Comisión:
   — recabará la opinión de los autores de la información clasificada cuya entrega se solicita,
   — entablará contactos preliminares con los órganos de seguridad del país o de la organización internacional solicitante, para recabar información sobre su política y normativa de seguridad y, en particular, para establecer un cuadro comparativo de las clasificaciones que se utilizan en la UE y en el país u organización interesado,
   — concertará una reunión del Grupo consultivo sobre política de seguridad de la Comisión o, si fuera necesario, mediante un procedimiento de aprobación tácita, recabará información de las ANS de los Estados miembros con el fin de obtener el dictamen del Grupo consultivo sobre política de seguridad de la Comisión.

5. El dictamen del Grupo consultivo sobre política de seguridad de la Comisión se referirá a lo siguiente:
   — la confianza que puede depositarse en los países u organizaciones internacionales beneficiarios, con el fin de evaluar los riesgos para la seguridad a que se expondrían la UE o sus Estados miembros,
   — una estimación de la capacidad de los beneficiarios para proteger la información clasificada entregada por la UE,
   — propuestas relativas a los procedimientos para la gestión de la información clasificada de la UE (por ejemplo, suministro de versiones expurgadas) y de los documentos transmitidos (mantenimiento o supresión de las rúbricas de la clasificación UE, de los marcados específicos, etc.);
   — recalificación o desclasificación antes de que la información se entregue a los países u organizaciones internacionales beneficiarios.

6. El miembro de la Comisión encargado de cuestiones de seguridad remitirá a la Comisión, para que ésta decida, la solicitud y el dictamen del Grupo consultivo sobre política de seguridad de la Comisión.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

7. El miembro de la Comisión encargado de cuestiones de seguridad notificará a los países u organizaciones internacionales beneficiarios, la decisión de la Comisión de autorizar la entrega de información clasificada de la UE, así como de sus restricciones.

8. La decisión de entregar la información no entrará en vigor hasta que los beneficiarios hayan dado garantías por escrito de que:
   — no utilizarán la información para fines distintos de los acordados,
   — protegerán la información de acuerdo con las normas establecidas por la Comisión.

9. Se establecerán las siguientes normas de protección, salvo en el caso de que la Comisión, después de recibir el dictamen técnico del Grupo consultivo sobre política de seguridad de la Comisión, decida un procedimiento especial para tratar los documentos clasificados de la UE (supresión de la mención de la clasificación de la UE, marcados específicos, etc.).

10. Personal

    a) El número de funcionarios con acceso a la información clasificada de la UE estará, según el principio de necesidad de conocer, estrictamente limitado a las personas cuyas funciones hagan necesario dicho acceso.

    b) Todos los funcionarios o ciudadanos autorizados a acceder a información clasificada entregada por la Comisión deberán estar en posesión de una habilitación de seguridad o autorización de acceso de rango nacional, respecto de información nacional clasificada, de un nivel adecuado equivalente al de la UE, tal como se define en el cuadro comparativo.

    c) Dichas habilitaciones de seguridad o autorizaciones nacionales se remitirán al Presidente a título informativo.

11. Transmisión de documentos

Los procedimientos prácticos para la transmisión de documentos se decidirán por acuerdo. En espera de la celebración de dicho acuerdo, serán aplicables las disposiciones de la sección 21. El acuerdo especificará en particular los registros a los que debe remitirse la información clasificada de la UE, las direcciones concretas a las que deben remitirse los documentos y los servicios de mensajería o correo utilizados para la transmisión de la información clasificada de la UE.

12. Registro de llegada

La ANS del país destinatario, o su equivalente en el país que recibe en nombre de su Gobierno información clasificada remitida por la Comisión, o bien el órgano de seguridad de la organización internacional receptora, tendrá un libro de registro especial para inscribir la información clasificada de la UE a su recepción. El libro de registro constará de columnas en las que se indicarán la fecha de recepción, la descripción del documento (fecha, referencia y número de copia), su clasificación, su título, el nombre o cargo del receptor, la fecha del acuse de recibo y la fecha de devolución del documento a la UE o de destrucción del mismo.

13. Devolución de documentos

Cuando el destinatario devuelva un documento clasificado a la Comisión, procederá en la forma que se indica en el apartado «Transmisión de documentos».

14. Protección

a) Cuando los documentos no se utilicen, se almacenarán en un contenedor de seguridad que habrá sido autorizado para contener el material nacional del mismo nivel de clasificación. El contenedor no llevará ninguna indicación de su contenido, que sólo será accesible a las personas autorizadas para tratar información clasificada de la UE. Cuando se utilicen cerraduras de combinación, dicha combinación sólo será conocida por los funcionarios del país u organización que tenga acceso autorizado a la información clasificada de la UE almacenada en el contenedor; se cambiará la combinación cada seis meses, o antes si se produce el traslado de un funcionario, si se retira la habilitación de seguridad de uno de los funcionarios que conocen la combinación o si existe riesgo de puesta en peligro.

b) Sólo podrán sacar del contenedor de seguridad los documentos clasificados de la UE los funcionarios habilitados para acceder a los documentos clasificados de la UE y que tengan necesidad de conocerlos. Serán responsables de la custodia y seguridad de dichos documentos durante todo el tiempo que éstos permanezcan en su poder y, en particular, deberán garantizar que ninguna persona no autorizada tenga acceso a los documentos. Deberán garantizar asimismo que los documentos queden almacenados en un contenedor de seguridad cada vez que hayan terminado de consultarlos y fuera de las horas de trabajo.

c) No podrán hacerse fotocopias de los documentos clasificados EU CONFIDENTIAL o de nivel superior, ni hacerse extractos sin la autorización de la Oficina de Seguridad de la Comisión.

d) El procedimiento para la destrucción rápida y total de los documentos en casos de urgencia deberá definirse y confirmarse conjuntamente con la Oficina de Seguridad de la Comisión.

15. Seguridad física

a) Cuando los documentos clasificados de la UE no se estén utilizando, los contenedores de seguridad empleados para almacenarlos se mantendrán cerrados en todo momento.

b) Cuando el personal de mantenimiento o de limpieza necesite entrar o trabajar en un local en el que se encuentren dichos contenedores de seguridad, deberá ir acompañado por un miembro del servicio de seguridad del país o de la organización, o por el funcionario más directamente responsable de supervisar la seguridad del local.

c) Fuera de los horarios normales de trabajo (por las noches, durante los fines de semana y en las vacaciones oficiales), los contenedores de seguridad que almacenen documentos clasificados de la UE estarán protegidos por un guardia o por un sistema de alarma automática.

16. Infracciones de la seguridad

Cuando se haya producido o se sospeche que se ha producido una infracción de la seguridad en relación con un documento clasificado de la UE, deberá actuarse inmediatamente de la siguiente forma:

a) remitir de inmediato un informe a la Oficina de Seguridad de la Comisión o a la ANS del Estado miembro que tomó la iniciativa de transmitir los documentos (con copia a la Oficina de Seguridad de la Comisión);

b) llevar a cabo una investigación, a cuyo término se remitirá un informe completo al órgano de seguridad [véase la letra a)]. A continuación deberán adoptarse las medidas necesarias para poner remedio a la situación.

17. Inspecciones

Se permitirá a la Oficina de Seguridad de la Comisión, previo acuerdo con los países u organizaciones internacionales interesados, evaluar la eficacia de las medidas destinadas a proteger la información clasificada de la UE que se entregue.

18. Informe

Sin perjuicio de que se celebre un acuerdo de seguridad, mientras el país u organización internacional tenga en su poder información clasificada de la UE, deberá presentar un informe anual en la fecha que se indique cuando se conceda la autorización para entregar información. En dicho informe se confirmará que se han cumplido las presentes normas de seguridad.

Apéndice 5

Directrices para la entrega de información clasificada de la UE a terceros países y Organizaciones Internacionales: cooperación de nivel 3

PROCEDIMIENTO

1. Ocasionalmente, la Comisión puede querer cooperar, en determinadas circunstancias especiales, con países u organizaciones que no pueden ofrecer las garantías exigidas por las presentes normas de seguridad; sin embargo, dicha cooperación puede requerir la entrega de información clasificada de la UE.

2. Recae en el autor la autoridad para entregar información clasificada de la UE a terceros países u organizaciones internacionales cuyas política y normativa de seguridad son notablemente distintas de las de la UE. Recae en el Colegio de Comisarios la autoridad para entregar información clasificada de la UE originada dentro de la Comisión.

   En principio, se limita a la información clasificada hasta el nivel EU SECRET inclusive, y no incluye la información clasificada protegida por indicaciones o marcados de seguridad especiales.

3. La Comisión estudiará la conveniencia de entregar información clasificada, evaluará la necesidad de conocerla que tienen los beneficiarios y decidirá acerca de la naturaleza de la información clasificada que pueda facilitarse.

4. Si la Comisión se muestra favorable, el miembro de la Comisión encargado de cuestiones de seguridad:
   — recabará la opinión de los autores de la información clasificada cuya entrega se solicite,
   — concertará una reunión del Grupo consultivo sobre política de seguridad de la Comisión o, si fuera necesario, mediante un procedimiento de aprobación tácita, recabará información de las ANS de los Estados miembros con el fin de obtener el dictamen del Grupo consultivo sobre política de seguridad de la Comisión.

5. El dictamen del Grupo consultivo sobre política de seguridad de la Comisión se referirá a lo siguiente:

   a) una evaluación de los riesgos relativos a la seguridad para la UE o sus Estados miembros;

   b) la clasificación de la información que puede entregarse;

   c) la recalificación o desclasificación de la información antes de entregarla;

   d) los procedimientos para tratar los documentos que hayan de entregarse (véase el siguiente apartado);

   e) los posibles métodos de transmisión (uso de servicios de correos públicos, sistemas de telecomunicaciones públicos o de seguridad, valija diplomática, correos habilitados, etc.).

6. Los documentos entregados a los países u organizaciones mencionados en el presente apéndice se prepararán, en principio, sin hacer referencia a su origen o a la clasificación de la UE. El Grupo consultivo sobre política de seguridad de la Comisión podrá recomendar:
   — la utilización de un marcado específico o de una clave,
   — la utilización de un sistema específico de clasificación que vincule la sensibilidad de la información con las medidas de control exigidas a los métodos de transmisión de documentos que usa el beneficiario.

7. El Presidente remitirá a la Comisión, para que ésta decida, el dictamen del Grupo consultivo sobre política de seguridad de la Comisión.

8. Una vez que la Comisión haya aprobado la entrega de información clasificada de la UE y los procedimientos prácticos de aplicación, la Oficina de Seguridad de la Comisión entablará los contactos necesarios con el órgano de seguridad del país u organización interesado para facilitar la aplicación de las medidas de seguridad previstas.

9. El miembro de la Comisión encargado de cuestiones de seguridad informará a los Estados miembros acerca de la naturaleza y clasificación de la información, y elaborará una relación de las organizaciones y países a los que dicha información puede entregarse, con arreglo a la decisión de la Comisión.

10. La Oficina de Seguridad de la Comisión adoptará todas las medidas necesarias para facilitar la evaluación de cualquier daño consiguiente y la revisión de los procedimientos.

    Siempre que se modifiquen las condiciones de la cooperación, la Comisión volverá a examinar la cuestión.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

11. El miembro de la Comisión encargado de cuestiones de seguridad notificará a los países u organizaciones internacionales beneficiarios de la decisión de la Comisión de autorizar la entrega de información clasificada de la UE, junto con las disposiciones detalladas de protección propuestas por el Grupo consultivo sobre política de seguridad de la Comisión aprobadas por la Comisión.

12. La decisión no entrará en vigor hasta que los beneficiarios hayan dado garantías por escrito de que:

— no utilizarán la información para fines distintos de la cooperación decidida por la Comisión,

— darán a la información la protección exigida por la Comisión.

13. Transmisión de documentos

a) Los procedimientos prácticos para la transmisión de documentos se decidirán por acuerdo entre la Oficina de Seguridad de la Comisión y los órganos de seguridad de los países u Organizaciones Internacionales destinatarios. Dichos procedimientos especificarán, en particular, las direcciones concretas a las que deben remitirse los documentos.

b) Los documentos clasificados EU CONFIDENTIAL y de nivel superior se transmitirán bajo doble pliego. El sobre interior llevará el sello específico o la clave acordada y una mención de la clasificación especial aprobada para el documento. Con cada documento clasificado se incluirá un impreso de recibo que no se clasificará como tal y que mencionará únicamente los datos del documento (referencia, fecha, número de copia) y su idioma, pero no el título.

c) El sobre interior se introducirá a continuación en el sobre exterior, que llevará un número de empaquetado a efectos de recepción. En el sobre exterior no figurará la clasificación de seguridad.

d) En cada caso se entregará a los correos un recibo en el que constará el número de empaquetado.

14. Registro de llegada

La ANS del país destinatario, o su equivalente en el país, que recibe en nombre de su Gobierno información clasificada remitida por la Comisión, o bien el órgano de seguridad de la organización internacional receptora, tendrá un libro de registro especial para inscribir la información clasificada de la UE a su recepción. El libro de registro constará de columnas en las que se indicarán la fecha de recepción, la descripción del documento (fecha, referencia y número de copia), su clasificación, su título, el nombre o cargo del receptor, la fecha del acuse de recibo y la fecha de devolución del documento a la UE o de destrucción del mismo.

15. Uso y protección de la información clasificada objeto de intercambio

a) La información clasificada EU SECRET será tratada por funcionarios especialmente designados, autorizados para acceder a la información con dicha clasificación. Se almacenará en armarios de seguridad de buena calidad, que sólo podrán ser abiertos por las personas autorizadas para acceder a la información que en ellos se contiene. Las zonas en que se sitúen dichos armarios estarán custodiadas permanentemente, y se instalará un sistema de comprobación para garantizar que sólo se permite la entrada a las personas debidamente autorizadas. La información clasificada EU SECRET se remitirá mediante valija diplomática, servicios de correo de seguridad y telecomunicaciones de seguridad. Sólo podrán hacerse copias de los documentos EU SECRET con el acuerdo escrito del autor. Todas las copias serán registradas y controladas. Se entregarán recibos de todas las operaciones relativas a los documentos clasificados EU SECRET.

b) La información clasificada EU CONFIDENTIAL será tratada por funcionarios debidamente designados, autorizados para recibir información en la materia. Los documentos se almacenarán en armarios de seguridad cerrados, en zonas controladas.

La información clasificada EU CONFIDENTIAL se remitirá mediante valija diplomática, servicios de correo militar y telecomunicaciones de seguridad. El organismo destinatario podrá hacer copias, cuyo número y distribución se inscribirán en registros especiales.

c) La información clasificada EU RESTRICTED se tratará en locales no accesibles a personas no autorizadas y se almacenará en armarios cerrados. Los documentos podrán remitirse mediante servicios públicos de correos como envío certificado en doble pliego y, en situaciones de urgencia durante operaciones en curso, mediante sistemas de telecomunicaciones públicos sin protección. Los destinatarios podrán hacer copias.

d) La información no clasificada no requerirá medidas especiales de protección y podrá remitirse por correo y por sistemas públicos de telecomunicaciones. Los destinatarios podrán hacer copias.

16. Destrucción

Los documentos que ya no sean necesarios deberán ser destruidos. Por lo que respecta a los documentos clasificados EU RESTRICTED y EU CONFIDENTIAL, se hará el apunte oportuno en los registros especiales. Por lo que respecta a los documentos clasificados EU SECRET, se expedirán certificados de destrucción firmados por dos personas que hayan presenciado su destrucción.

17. Infracciones de seguridad

Si la información clasificada EU CONFIDENTIAL o EU SECRET se viera en peligro o si existiera la sospecha de que podría verse en peligro, la ANS del país o el jefe de seguridad de la organización llevará a cabo una investigación sobre las circunstancias del riesgo. Se informará a la Oficina de Seguridad de la Comisión acerca de sus resultados. Deberán adoptarse las medidas necesarias para subsanar procedimientos o métodos de almacenamiento inadecuados, si han dado origen a un riesgo.

Apéndice 6

LISTA DE ABREVIATURAS

ANS	Autoridad nacional de seguridad
CCCC	Comisión Consultiva de Compras y Contratos
CISO	Responsable central de seguridad informática
COMPUSEC	Seguridad de los ordenadores
COMSEC	Seguridad de las comunicaciones
CSO	Oficina de Seguridad de la Comisión
ESDP	Política europea común de seguridad y de defensa
IA	Autoridad INFOSEC
INFOSEC	Seguridad de la información
IO	Propietario de la información
ISO	Organización Internacional de Normalización
LISO	Responsable local de seguridad informática
LSO	Responsable local de seguridad
MSO	Responsable de seguridad de reunión
PC	Ordenador personal
RCO	Controlador de registro
SAA	Autoridad de acreditación en materia de seguridad
SecOPS	Procedimientos operativos de seguridad
SSRS	Requisitos específicos de seguridad del sistema
TI	Tecnología de la información
TSO	Propietario de los sistemas técnicos