II

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

CONSEJO

DECISIÓN DEL CONSEJO

de 19 de marzo de 2001

por la que se adoptan las normas de seguridad del Consejo

(2001/264/CE)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 3 de su artículo 207,

Vista la Decisión 2000/396/CE, CECA, Euratom del Consejo, de 5 de junio de 2000, por la que se adopta su Reglamento interno [1] y, en particular, su artículo 24,

Considerando lo siguiente:

(1) A fin de desarrollar las actividades del Consejo en ámbitos que exigen determinado grado de confidencialidad, es conveniente establecer un sistema exhaustivo de seguridad que abarque el Consejo, su Secretaría General y los Estados miembros.

(2) Dicho sistema deberá combinar en un texto único la temática cubierta por todas las decisiones y disposiciones anteriores en la misma materia.

(3) En la práctica, la mayor parte de la información de la UE clasificada «CONFIDENTIEL UE» y de nivel superior se referirá a la Política Común de Seguridad y Defensa.

(4) A fin de salvaguardar la eficacia del sistema de seguridad así establecido, los Estados miembros deberán quedar asociados a su funcionamiento mediante la adopción de las medidas nacionales necesarias para cumplir las disposiciones de la presente Decisión en aquellos casos en que sus autoridades y funcionarios competentes traten información clasificada de la UE.

(5) El Consejo acoge favorablemente la intención de la Comisión de instaurar, a más tardar en la fecha de aplicación de la presente Decisión, un sistema exhaustivo que esté en consonancia con los anexos de la misma, con miras a garantizar el buen funcionamiento del proceso de toma de decisiones en la Unión.

(6) El Consejo subraya la importancia de que, cuando resulte adecuado, el Parlamento Europeo y la Comisión queden asociados a las reglas y normas de confidencialidad que son necesarias para proteger los intereses de la Unión y de sus Estados miembros.

(7) La presente Decisión se adopta sin perjuicio de lo dispuesto en el artículo 255 del Tratado y de sus instrumentos de aplicación.

(8) La presente Decisión se adopta sin perjuicio de las prácticas vigentes en los Estados miembros respecto de la información sobre las actividades de la Unión a sus Parlamentos nacionales respectivos,

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Quedan aprobadas las normas de seguridad del Consejo recogidas en el anexo.

Artículo 2

1. El Secretario General/Alto Representante adoptará las medidas adecuadas para garantizar que, al tratar información clasificada de la UE, las normas a que se refiere el artículo 1 sean cumplidas en la Secretaría General del Consejo (en lo sucesivo, «SGC») tanto por los funcionarios y otros agentes de la SGC como por los contratistas externos de la SGC y por el personal enviado a la SGC en comisión de servicio, así como en los locales del Consejo y en los organismos descentralizados de la UE [2].

[1] DO L 149 de 23.6.2000, p. 21.

[2] Véanse las Conclusiones del Consejo de 10 de noviembre de 2000.

2. Los Estados miembros adoptarán, de conformidad con sus disposiciones nacionales, las medidas adecuadas para garantizar que, cuando se trate información clasificada de la UE, las normas a que se refiere el artículo 1 sean cumplidas, dentro de sus servicios y locales:

a) por los miembros de las Representaciones Permanentes de los Estados miembros ante la UE, así como por los miembros de las Delegaciones nacionales que asistan a reuniones del Consejo o de sus órganos, o que participen en otras actividades del Consejo,

b) por 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, y

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

Los Estados miembros informarán inmediatamente a la SGC de las medidas adoptadas.

3. Las medidas mencionadas en los apartados 1 y 2 se adoptarán antes del 30 de noviembre de 2001.

Artículo 3

En consonancia con los principios básicos y normas mínimas de seguridad que figuran en la parte I del anexo, el Secretario General/Alto Representante podrá adoptar medidas con arreglo a lo dispuesto en los apartados 1 y 2 de la sección I de la parte II del anexo.

Artículo 4

La presente Decisión sustituirá, a partir de la fecha de su aplicación, a las siguientes:

a) Decisión 98/319/CE del Consejo, de 27 de abril de 1998, relativa a las normas con arreglo a las cuales los funcionarios y agentes de la SGC podrán ser autorizados a tener acceso a información clasificada en poder del Consejo [1],

b) Decisión del Secretario General del Consejo/Alto Representante para la política exterior y de seguridad común, de 27 de julio de 2000, relativa a las medidas de protección de la información clasificada aplicables en la Secretaría General del Consejo [2];

c) Decisión 433/97 de la Secretaría General del Consejo, de 22 de mayo de 1997, relativa al procedimiento de investigación de los funcionarios responsables del funcionamiento del sistema Cortesy.

Artículo 5

1. La presente Decisión entrará en vigor en la fecha de su publicación.

2. Se aplicará a partir del 1 de diciembre de 2001.

Hecho en Bruselas, el 19 de marzo de 2001.

Por el Consejo

El Presidente

A. LINDH

[1] DO L 140 de 12.5.1998, p. 12.

[2] DO C 239 de 23.8.2000, p. 1.

ANEXO

NORMAS DE SEGURIDAD DEL CONSEJO DE LA UNIÓN EUROPEA

ÍNDICE

Página

PARTE I

Principios básicos y normas mínimas de seguridad 6

PARTE II 10

SECCIÓN I

La organización de la seguridad en el Consejo de la Unión Europea 10

SECCIÓN II

Clasificaciones y marcados 12

SECCIÓN III

Gestión de la clasificación 13

SECCIÓN IV

Seguridad física 14

SECCIÓN V

Normas generales sobre el principio de necesidad de conocer y la habilitación de seguridad 18

SECCIÓN VI

Procedimiento de habilitación de seguridad aplicable a los funcionarios y otros agentes de la SGC 20

SECCIÓN VII

Elaboración, distribución, transmisión, almacenamiento y destrucción de material clasificado de la UE 22

SECCIÓN VIII

Registros TRÈS SECRET UE/EU TOP SECRET 29

SECCIÓN IX

Medidas de seguridad que deberán aplicarse con motivo de la celebración de reuniones específicas, fuera de los locales del Consejo, que se refieran a asuntos muy sensibles 31

SECCIÓN X

Quebrantamientos de la seguridad y puesta en peligro de información clasificada de la UE 34

SECCIÓN XI

Protección de la información tratada en los sistemas de tecnología de la información y de comunicación 36

SECCIÓN XII

Entrega de información clasificada de la UE a terceros países u organizaciones internacionales 48

Página

Apéndices

Apéndice 1

Lista de autoridades nacionales de seguridad 50

Apéndice 2

Comparación de las clasificaciones de seguridad nacionales 53

Apéndice 3

Guía práctica de clasificación 54

Apéndice 4

Directrices para la entrega de información clasificada de la UE a terceros países u organizaciones internacionales — Cooperación de nivel 1 58

Apéndice 5

Directrices para la entrega de información clasificada de la UE a terceros países u organizaciones internacionales — Cooperación de nivel 2 61

Apéndice 6

Directrices para la entrega de información clasificada de la UE a terceros países u organizaciones internacionales — Cooperación de nivel 3 64

PARTE I

PRINCIPIOS BÁSICOS Y NORMAS MÍNIMAS DE SEGURIDAD

INTRODUCCIÓN

1. Las presentes disposiciones establecen los principios básicos y las normas mínimas de seguridad que deberán respetar de manera adecuada el Consejo, la Secretaría General del Consejo (en lo sucesivo, «SGC»), los Estados miembros y los organismos descentralizados de la Unión Europea (en lo sucesivo, «organismos descentralizados de la UE»), a fin de salvaguardar la seguridad y de garantizarles el establecimiento de una norma común de protección.

2. Por «información clasificada de la UE» se entenderá toda información y material cuya divulgación no autorizada pueda causar perjuicio en distintos grados a los intereses de la UE, o de uno o más de sus Estados miembros, ya se origine dicha información dentro de la UE o se reciba de Estados miembros, terceros países u organizaciones internacionales.

3. En las presentes normas se entenderá por:

   a) «documento» todo escrito, nota, acta, informe, memorándum, señal/mensaje, dibujo, fotografía, diapositiva, película, mapa, carta de navegación, 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;

   b) «material» todo «documento» según se define en la anterior letra a), así como todo artículo de equipo o armamento, producido o en proceso de producción.

4. La seguridad tiene 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 integridad y disponibilidad;

   c) proteger las instalaciones que albergan 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 necesarias medidas para remediarlo.

5. Los fundamentos de una óptima seguridad son los siguientes:

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

      i) la recopilación y registro de información confidencial en materia de espionaje, sabotaje, terrorismo y otras actividades subversivas;

      ii) la información y el asesoramiento facilitados a su correspondiente Gobierno y, a través de él, al Consejo, sobre la índole de las amenazas contra la seguridad y sobre los medios de protección frente a dichas amenazas;

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

   c) una colaboración habitual entre los ministerios, los organismos y los servicios adecuados de la SGC para determinar y recomendar, según resulte apropiado:

      i) qué información, recursos e instalaciones requieren protección; y

      ii) unas normas comunes de protección.

6. Por lo que atañe a la confidencialidad, se requiere cuidado y experiencia a la hora de seleccionar la información y el material que debe protegerse, así como a la hora de evaluar el grado de protección requerido. Resulta fundamental que el grado de protección se corresponda con el resultado de la evaluación crítica en materia de seguridad del elemento concreto de información y material que haya de protegerse. A fin de garantizar que la información circule adecuadamente, se tomarán medidas para evitar la clasificación excesiva. El sistema de clasificación es el instrumento que permite poner en vigor estos principios; deberá seguirse un sistema de clasificación similar a la hora de planificar y organizar los medios para contrarrestar el espionaje, el sabotaje, el terrorismo y otras amenazas, otorgando el mayor grado de protección a los locales más importantes que alberguen información clasificada y, dentro de ellos, a los puntos más sensibles.

PRINCIPIOS BÁSICOS

7. **Las medidas de seguridad deberán:**

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

b) concebirse de manera tal que permitan detectar a aquellas personas cuya situación pueda poner en peligro la seguridad de la información clasificada y de instalaciones importantes que contengan información clasificada, y facilitar la exclusión o cese de las mismas;

c) impedir que personas no autorizadas tengan acceso a la información clasificada o a las instalaciones que la contengan;

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 de la seguridad;

e) garantizar la integridad (es decir, impedir la alteración o 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.

LA ORGANIZACIÓN DE LA SEGURIDAD

Normas mínimas comunes

8. El Consejo y cada uno de los Estados miembros garantizarán la observancia de normas mínimas de seguridad comunes en todos los departamentos administrativos y/o ministeriales, así como en otras instituciones, organismos y contratistas de la UE, a fin de que la información clasificada de la UE pueda transmitirse con la confianza de que se tratará con idéntico cuidado. Estas normas mínimas incluirán criterios para la habilitación de seguridad del personal, así como procedimientos para la protección de la información clasificada de la UE.

SEGURIDAD DEL PERSONAL

Habilitación del personal

9. Todas las personas que necesiten acceder a la información clasificada CONFIDENTIEL UE 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 aquellas 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; o

c) pueden resultar vulnerables a presiones de fuentes extranjeras o de otras fuentes, por ejemplo a causa de su anterior residencia o de antiguas relaciones que pudieran constituir un riesgo para la seguridad.

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

d) a las que se haya de conceder acceso a la información clasificada TRÈS SECRET UE/EU TOP SECRET;

e) que ocupen puestos que traigan aparejado el acceso habitual a un volumen considerable de información clasificada SECRET UE;

f) cuyas obligaciones les den especial acceso a sistemas de comunicación o información de importancia fundamental para una misión y que tengan así la posibilidad de obtener acceso no autorizado a grandes cantidades de información clasificada de la UE, o de infligir un grave daño a la misión de que se trate mediante actos de sabotaje técnico.

En las circunstancias expuestas en las anteriores letras d), e) y f), se recurrirá en el grado más amplio que resulte viable a la técnica de investigación de antecedentes.

10. Cuando haya de recurrirse 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 limpiadores, etc.), dichas personas se someterán previamente al debido procedimiento de habilitación de seguridad.

Registros de habilitaciones del personal

11. Todos los servicios, órganos o instituciones que traten información clasificada de la UE o alberguen sistemas de comunicación e información de importancia fundamental para una misión deberán mantener un registro de las habilitaciones concedidas al personal que tengan asignado. Cada habilitación de seguridad deberá verificarse, cuando la ocasión lo exija, con objeto de garantizar que resulta adecuada para la asignación actual de la persona de que se trate; la habilitación deberá volver a examinarse prioritariamente 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 de la seguridad. El jefe de seguridad del servicio, órgano o institución de que se trate mantendrá el registro de habilitaciones de seguridad.

Instrucción del personal en materia de seguridad

12. 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 la necesidad de la seguridad y los procedimientos para conseguirla. Resulta útil el procedimiento de exigir que todo el personal de esta índole certifique por escrito la plena comprensión de las normas de seguridad correspondientes al puesto que se le haya asignado.

Responsabilidades de gestión

13. 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 importancia fundamental para una misión, así como de registrar y comunicar cuantos incidentes o aparentes muestras de vulnerabilidad puedan afectar a la seguridad.

Estatuto de seguridad del personal

14. Deberán establecerse procedimientos para garantizar que, cuando se entre en conocimiento de información negativa en relación con una persona, se determine si ésta trabaja con información clasificada o tiene acceso a sistemas de comunicación o información de importancia fundamental para una misión, y se informe a la autoridad correspondiente. En caso de que se determine que una persona constituye un riesgo para la seguridad, se la excluirá o cesará de aquellos puestos en los que pueda poner en peligro la seguridad.

SEGURIDAD FÍSICA

Necesidad de protección

15. El grado de las medidas de seguridad física que deberá aplicarse para garantizar la protección de información clasificada de la UE deberá ser proporcional al nivel de clasificación, al volumen de la información y a la amenaza a que se expongan la información y el material de que se trate. Así pues, deberán evitarse cuidadosamente tanto la clasificación excesiva como la insuficiente, y la clasificación deberá someterse a una revisión periódica. Todas las personas que estén en posesión de información clasificada de la UE deberán seguir 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.

Comprobación

16. Antes de dejar sin vigilancia los lugares que contengan 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 de que todos los dispositivos de seguridad hayan sido activados (cerraduras, alarmas, etc.). Después de las horas de trabajo deberán llevarse a cabo otros controles independientes.

Seguridad de los edificios

17. Los edificios que alberguen información clasificada de la UE o sistemas de comunicación e información de importancia fundamental para una misión deberán estar protegidos contra el acceso no autorizado. La índole de la protección dada 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, dependerán de:

a) la clasificación, el volumen y la ubicación dentro del edificio de la información y del material que deba protegerse;

b) la calidad de los contenedores de seguridad destinados a esta información y material; y

c) la naturaleza física y la ubicación del edificio.

18. La índole de la protección dada a los sistemas de comunicación e información dependerá, de modo similar, de una evaluación de la importancia de los efectos que deban protegerse y de los posibles daños que se derivarían en caso de que la seguridad se viera en peligro, así como de la naturaleza física y de la ubicación del edificio que albergue el sistema, y de la ubicación del sistema dentro del edificio.

Planes de emergencia

19. Deberán prepararse con antelación planes detallados para la protección de la información clasificada durante una emergencia local o nacional.

SEGURIDAD DE LA INFORMACIÓN (INFOSEC)

20. 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 en sistemas de comunicación, de información y otros sistemas electrónicos frente a la pérdida de confidencialidad, integridad o disponibilidad de la misma, ya sea accidental o intencionada. Deberán adoptarse las contramedidas adecuadas para impedir el acceso de usuarios no autorizados a la información de la UE, para impedir la denegación de acceso a información de la UE a usuarios autorizados y para impedir la deformación, modificación o borrado no autorizados de información de la UE.

LUCHA CONTRA EL SABOTAJE Y OTRAS FORMAS DE DAÑO INTENCIONADO

21. Las precauciones físicas para la protección de instalaciones importantes que alberguen información clasificada constituyen las mejores salvaguardias de seguridad para protegerla contra el sabotaje y los daños intencionados, sin que la mera habilitación del personal pueda sustituirlas de manera eficaz. El órgano nacional competente deberá recoger información confidencial relativa al espionaje, el sabotaje, el terrorismo y otras actividades subversivas.

ENTREGA DE INFORMACIÓN CLASIFICADA A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

22. Corresponderá al Consejo adoptar la decisión de difundir a un tercer país u organización internacional información clasificada originada en el Consejo. En caso de que el emisor de la información cuya entrega se desea no sea el Consejo, éste deberá recabar el consentimiento del emisor antes de difundirla. En caso de que no sea posible determinar el emisor, el Consejo asumirá la responsabilidad de aquél.

23. En caso de que el Consejo reciba información clasificada procedente de terceros países, organizaciones internacionales u otros terceros, se dará a dicha información la protección adecuada a su clasificación y equivalente a la de los niveles establecidos en las presentes normas para la información clasificada de la UE o a los niveles de grado superior que pueda exigir el tercero que difunda la información. Podrán disponerse controles mutuos.

24. Los principios que anteceden se aplicarán de conformidad con las normas de desarrollo recogidas en la parte II.

PARTE II

SECCIÓN I

LA ORGANIZACIÓN DE LA SEGURIDAD EN EL CONSEJO DE LA UNIÓN EUROPEA

El Secretario General/Alto Representante

1. El Secretario General/Alto Representante:

   a) aplicará la política de seguridad del Consejo;

   b) considerará los problemas de seguridad que le transmitan el Consejo o sus órganos competentes;

   c) examinará las cuestiones que impliquen cambios en la política de seguridad del Consejo, en estrecha colaboración con las Autoridades Nacionales de Seguridad (en lo sucesivo, «ANS») de los Estados miembros, u otras autoridades apropiadas. En el apéndice 1 figura una lista de dichas autoridades.

2. En particular, el Secretario General/Alto Representante será responsable de:

   a) coordinar todos los asuntos de seguridad relativos a las actividades del Consejo;

   b) solicitar a cada Estado miembro que establezca un registro central TRÈS SECRET UE/EU TOP SECRET y requerir la creación de dicho registro en los organismos descentralizados de la UE, según resulte adecuado;

   c) dirigir solicitudes a las autoridades designadas de los Estados miembros con objeto de que las ANS faciliten habilitaciones de seguridad para el personal empleado en la SGC, de conformidad con lo dispuesto en la Sección VI;

   d) investigar u ordenar que se realice una investigación sobre cualquier fuga de información clasificada de la UE que, según indicios razonables pero no concluyentes, se haya producido en la SGC o en cualquiera de los organismos descentralizados de la UE;

   e) solicitar a las autoridades de seguridad adecuadas que emprendan investigaciones cuando una fuga de información clasificada de la UE parezca haberse producido fuera de la SGC o de los organismos descentralizados de la UE, y coordinar las indagaciones en caso de que más de una autoridad de seguridad participe en las mismas;

   f) llevar a cabo, conjuntamente y de acuerdo con las ANS interesadas, exámenes periódicos de las disposiciones de seguridad para la protección de la información clasificada de la UE en los Estados miembros;

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

   h) mantener bajo constante revisión la política y los procedimientos de seguridad del Consejo y, en caso necesario, preparar las recomendaciones adecuadas. A este respecto, deberá presentar al Consejo el plan anual de inspección preparado por la Oficina de Seguridad de la SGC.

El Comité de Seguridad del Consejo

3. Se creará un Comité de Seguridad, que estará integrado por representantes de la ANS de cada Estado miembro. Estará presidido por el Secretario General/Alto Representante o por la persona en quien éste delegue. También podrá invitarse a representantes de los organismos descentralizados de la UE a asistir a las reuniones cuando se debatan cuestiones que les afecten.

4. El Comité de Seguridad se reunirá siguiendo instrucciones del Consejo, a instancias del Secretario General/Alto Representante o de una ANS. Estará facultado para examinar y evaluar todas las cuestiones de seguridad relativas a los trabajos del Consejo y para representar al Consejo las recomendaciones que procedan. Por lo que respecta a la actividad de la SGC, el Comité estará facultado para formular recomendaciones sobre cuestiones de seguridad al Secretario General/Alto Representante.

La Oficina de Seguridad de la SGC

5. A fin de ejercer las competencias mencionadas en los apartados 1 y 2, el Secretario General/Alto Representante dispondrá de la Oficina de Seguridad de la SGC para coordinar, supervisar y aplicar las medidas de seguridad.

6. El jefe de la Oficina de Seguridad de la SGC será el principal asesor del Secretario General/Alto Representante en materia de seguridad y actuará como secretario del Comité 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 al Consejo por acuerdos de seguridad. A estos efectos, actuará en calidad de funcionario de enlace.

7. El jefe de la Oficina de Seguridad de la SGC será responsable de la acreditación de los sistemas y redes de tecnología de la información (en lo sucesivo, «TI») dentro de la SGC. El jefe de la Oficina de Seguridad de la SGC y la ANS correspondiente decidirán conjuntamente, cuando proceda, en materia de acreditación de los sistemas y redes de TI en los que participen la SGC, los Estados miembros, los organismos descentralizados de la UE o terceros (Estados u organizaciones internacionales).

Organismos descentralizados de la UE

8. Cada director de un organismo descentralizado de la UE será responsable de llevar a efecto la seguridad dentro de su centro. Normalmente, nombrará a un miembro de su personal que será responsable ante él en este ámbito, y al que se designará funcionario de seguridad.

Estados miembros

9. Cada Estado miembro designará a un responsable de la ANS para la seguridad de la información clasificada de la UE [1].

10. En el marco de cada administración de los Estados miembros, la ANS correspondiente será responsable de:

    a) mantener la seguridad de la información clasificada de la UE que esté en posesión de cualquier departamento, órgano u organismo nacional, de carácter público o privado, en el territorio nacional o en el extranjero;

    b) autorizar la creación de registros TRÈS SECRET UE/EU TOP SECRET (esta facultad podrá delegarse en el controlador TRÈS SECRET UE/EU TOP SECRET de un registro central);

    c) inspeccionar periódicamente las disposiciones de seguridad para la protección de la información clasificada de la UE;

    d) garantizar que todos los nacionales y todos los extranjeros empleados en un departamento, órgano u organismo nacional que puedan tener acceso a información de la UE clasificada TRÈS SECRET UE/EU TOP SECRET, SECRET UE y CONFIDENTIEL UE se hayan sometido a investigaciones de seguridad;

    e) elaborar los planes de seguridad que se consideren necesarios para impedir que la información clasificada de la UE caiga en manos de personas no autorizadas.

Inspecciones mutuas de seguridad

11. La Oficina de Seguridad de la SGC y la ANS correspondiente llevarán a cabo, conjuntamente y de común acuerdo, inspecciones periódicas de las disposiciones de seguridad para la protección de la información clasificada de la UE en la SGC y en las Representaciones Permanentes de los Estados miembros ante la UE, así como en los locales destinados a los Estados miembros en los edificios del Consejo [2].

12. La Oficina de Seguridad de la SGC o, a instancias del Secretario General/Alto Representante, la ANS del Estado miembro anfitrión llevarán a cabo inspecciones periódicas de las disposiciones de seguridad para la protección de la información clasificada de la UE en los organismos descentralizados de la UE.

---

[1] En el Apéndice 1 se recoge una lista de las ANS responsables de la seguridad de la información clasificada de la UE.

[2] Sin perjuicio de la Convención de Viena de 1961 sobre relaciones diplomáticas.

SECCIÓN II

CLASIFICACIONES Y MARCADOS

NIVELES DE CLASIFICACIÓN [1]

La información se clasificará en los siguientes niveles:

1. TRÈS SECRET UE/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.

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

3. CONFIDENTIEL UE: 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.

4. RESTREINT UE: 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.

MARCADOS

5. Podrá utilizarse un marcado de advertencia para especificar el ámbito abarcado por el documento o para indicar una distribución específica basada en el principio de necesidad de conocer.

6. El marcado ESDP/PESD 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.

7. Determinados documentos, como los relativos a los sistemas de TI, podrán llevar un marcado adicional que implique medidas de seguridad suplementarias definidas en la normativa correspondiente.

ESTAMPACIÓN DE LA CLASIFICACIÓN Y DE LOS MARCADOS

8. La clasificación y los marcados se indicarán del siguiente modo:

   a) en los documentos RESTREINT UE, por medios mecánicos o electrónicos;

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

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

[1] En el Apéndice 2 se recoge un cuadro comparativo de los niveles de seguridad de la UE, la OTAN, la UEO y los Estados miembros.

SECCIÓN III

GESTIÓN DE LA CLASIFICACIÓN

1. 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.

2. El único responsable de la clasificación de la información y de cualquier recalificación o desclasificación ([1]) que se produzca posteriormente será el emisor.

   Los funcionarios y otros agentes de la SGC clasificarán, recalificarán o desclasificarán la información siguiendo instrucciones de su Director General o con su consentimiento.

3. Los procedimientos precisos para el tratamiento de los documentos clasificados habrán sido concebidos para garantizar la protección adecuada de la información contenida en ellos.

4. Se reducirá al mínimo el número de personas autorizadas a emitir documentos TRÈS SECRET UE/EU TOP SECRET y sus nombres se registrarán en una lista elaborada por la SGC, cada Estado miembro y, en su caso, cada organismo descentralizado de la UE.

APLICACIÓN DE LAS CLASIFICACIONES

5. La clasificación de un documento se determinará con arreglo al nivel de sensibilidad de su contenido, de acuerdo con la definición de los apartados 1 a 4 de la sección II. Es importante que la clasificación se utilice correctamente y con moderación, en particular en el caso de la clasificación TRÈS SECRET UE/EU TOP SECRET.

6. El emisor de un documento que se vaya a clasificar deberá tener en cuenta las normas expuestas y frenar cualquier tendencia a clasificar de forma excesiva o insuficiente.

   Aunque un elevado nivel de clasificación puede dar la impresión, a primera vista, de proteger con mayor eficacia un documento, si rutinariamente se clasifica en forma excesiva se puede producir una pérdida de confianza en la validez del sistema de clasificación.

   Por el contrario, los documentos no deben clasificarse de forma insuficiente con el fin de evitar las limitaciones que conlleva la protección.

   En el apéndice 3 figura una guía práctica de la clasificación.

7. 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 será equivalente a la de la parte clasificada al nivel más alto.

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

RECALIFICACIÓN Y DESCLASIFICACIÓN

9. Los documentos clasificados de la UE podrán recalificarse o desclasificarse únicamente con la autorización del emisor y, en caso necesario, tras consultar a las demás partes interesadas. La recalificación o desclasificación se confirmarán por escrito. La institución, Estado miembro, oficina, organización sucesora o autoridad superior de emisión 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.

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

([1]) Se entenderá por recalificación *(downgrading-déclassement)* la disminución del nivel de clasificación. Se entenderá por desclasificación *(declassification – déclassification)* la supresión de toda mención de clasificación.

SECCIÓN IV

SEGURIDAD FÍSICA

GENERAL

1. El objetivo principal de las medidas de seguridad física es impedir que una persona no autorizada acceda a información o material clasificados de la UE.

REQUISITOS DE SEGURIDAD

2. 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.

3. Al decidir el grado de protección de la 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 guarda;

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

4. Las medidas de seguridad física aplicadas se concebirán con vistas a:

   a) impedir la entrada subrepticia o forzada de intrusos;

   b) disuadir, dificultar y detectar acciones de personal desleal (el espía de dentro);

   c) impedir el acceso no justificado a información clasificada de la UE por parte de funcionarios y otros agentes de la SGC, de las administraciones nacionales de los Estados miembros y de otras instituciones o terceros.

MEDIDAS FÍSICAS DE SEGURIDAD

Zonas de Seguridad

5. Las zonas en que se trate y almacene información clasificada CONFIDENTIEL UE 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 CONFIDENTIEL UE, de manera que la entrada en dicha zona constituye, a todos los efectos prácticos, un acceso a información clasificada. Esta 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 entrada que admita únicamente a las personas con permiso válido y autorizadas especialmente a entrar en la zona;

      iii) una especificación de la clasificación de la información que habitualmente se contenga en la zona, como, por ejemplo, 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 CONFIDENTIEL UE o de nivel superior de manera que pueda protegerse del acceso de personas no autorizadas mediante controles internos, por ejemplo, los locales con oficinas en las que se almacena y trata habitualmente información CONFIDENTIEL UE. 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 entrada en la que sólo puedan entrar 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.

Zona Administrativa

6. Se podrán crear zonas administrativas o 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 RESTREINT UE.

Controles de entrada y salida

7. La entrada a las zonas de seguridad de Clase I y Clase II se controlará mediante un pase o sistema de reconocimiento personal aplicable al personal permanente. Igualmente se creará un sistema de comprobación de visitantes que permita denegar el acceso no autorizado a la información clasificada de la UE. Los sistemas de los pases podrán basarse en una identificación automatizada que se considerará adicional a los guardias, pero nunca totalmente sustitutiva de éstos. Una modificación de las posibilidades de riesgo podrá conllevar el refuerzo de las medidas de control de entradas y salidas, por ejemplo con motivo de la visita de una persona importante.

Patrullas de guardia

8. 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.

Contenedores de seguridad y cámaras acorazadas

9. Para almacenar información clasificada de la UE se utilizarán tres clases de contenedores:

   — Clase A: contenedores con homologación nacional para el almacenamiento de información TRÈS SECRET UE/EU TOP SECRET dentro de una zona de seguridad de Clase I o Clase II;

   — Clase B: contenedores con homologación nacional para el almacenamiento de información SECRET UE y CONFIDENTIEL UE dentro de una zona de seguridad de Clase I o Clase II;

   — Clase C: mobiliario de oficina adecuado para guardar información RESTREINT UE únicamente.

10. 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 CONFIDENTIEL UE y de nivel superior en estanterías abiertas o desplegada en forma de cartas, mapas, etc., una ANS deberá certificar que las paredes, suelos y techos y puertas con cerradura ofrecen un nivel de protección equivalente al de la clase de contenedor de seguridad homologado para el almacenamiento de información de la misma clasificación.

Cerraduras

11. Las cerraduras utilizadas en los contenedores 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 contenedores de la Clase A;

   — Grupo B: homologación nacional para contenedores de la Clase B;

   — Grupo C: válido únicamente para mobiliario de oficina de la Clase C.

Control de las llaves y las combinaciones

12. Las llaves de los contenedores de seguridad no se sacarán del edificio en el que se encuentren las oficinas. Se encargarán de fijar y memorizar las combinaciones de los contenedores de seguridad las personas que necesiten conocerlas. El agente de seguridad encargado de los locales será responsable de custodiar 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 contenedores 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.

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

a) cada vez que se reciba un nuevo contenedor;

b) cada vez que haya un cambio de personal;

c) cada vez que se haya producido o se haya sospechado que se ha producido una situación de peligro;

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

Dispositivos de detección de intrusos

14. 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 red general. También existirá un sistema de alarma u otro tipo de aviso fiable al personal de vigilancia en caso de funcionamiento incorrecto o de intento de manipulación de los citados sistemas.

Equipo homologado

15. Las ANS mantendrán, procedentes de recursos propios o bilaterales, listas actualizadas por tipo y modelo del equipo de seguridad homologado por ellas para la protección directa o indirecta de información clasificada en diferentes circunstancias y condiciones especificadas. La Oficina de Seguridad de la SGC tendrá también una lista similar, basada, entre otras fuentes, en información facilitada por las ANS. Los organismos descentralizados de la UE consultarán a la Oficina de Seguridad de la SGC y, en su caso, a las ANS de su Estado anfitrión, antes de comprar equipo de estas características.

Protección física de las copiadoras y de los telefax

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

PROTECCIÓN CONTRA LA OBSERVACIÓN Y LA ESCUCHA

Observación

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

Escucha

18. Las oficinas y zonas en que se hable habitualmente sobre información clasificada SECRET UE o de nivel superior estarán protegidas contra la escucha pasiva y activa siempre que exista un riesgo que así lo exija. Será responsable de la evaluación de este riesgo la autoridad competente en materia de seguridad, tras consultar, en caso necesario, a las ANS.

19. 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 filtraciones peligrosas), así como a escucha activa (búsqueda de micrófonos, por ejemplo), la SGC podrá solicitar asistencia de expertos de las ANS. Los encargados de la seguridad de los organismos descentralizados de la UE podrán solicitar que la Oficina de Seguridad de la SGC efectúe inspecciones técnicas o la asistencia de expertos de las ANS, o ambas cosas.

20. 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 SECRET UE o superior podrán someterse a comprobación por parte de especialistas técnicos en materia de seguridad de las ANS, a petición del agente de seguridad competente.

ZONAS TÉCNICAMENTE SEGURAS

21. Determinadas zonas podrán designarse zonas técnicamente seguras. Se efectuará una comprobación especial a la 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 regulares, que podrán realizarse igualmente en caso de entrada o de sospecha de entrada de cualquier persona no autorizada.

22. Se realizará un inventario detallado del equipo y mobiliario a fin de seguir sus movimientos. No se introducirá en esta zona ningún mueble o equipo que no haya sido minuciosamente inspeccionado por personal de seguridad preparado especialmente para detectar cualquier dispositivo de escucha. Por norma general, se deberá evitar la instalación de cables de comunicación en zonas técnicamente seguras.

SECCIÓN V

NORMAS GENERALES SOBRE EL PRINCIPIO DE NECESIDAD DE CONOCER Y LA HABILITACIÓN DE SEGURIDAD

1. Se autorizará el acceso a la información clasificada de la UE únicamente a las personas para las que se justifique por motivo de su tarea o misión. El acceso a la información clasificada TRÈS SECRET UE/EU TOP SECRET, SECRET UE y CONFIDENTIEL UE sólo se autorizará a las personas que posean la debida habilitación de seguridad.

2. La responsabilidad de determinar si se justifica el conocimiento de la información clasificada corresponderá a la SGC, a los organismos descentralizados de la UE y a los servicios o departamentos del Estado miembro en que la persona de que se trate vaya a trabajar, en función de los requisitos de su tarea.

3. La habilitación del personal será responsabilidad del empleador del funcionario con arreglo a los procedimientos aplicables correspondientes. En el caso de los funcionarios y otros agentes de la SGC, se seguirá el procedimiento de habilitación de seguridad previsto en la sección VI.

   Tras el procedimiento citado se expedirá 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 a información clasificada de nivel inferior.

4. Las personas que no sean funcionarios u otros agentes de la SGC o de los Estados miembros, por ejemplo diputados, funcionarios o agentes de instituciones de la UE, 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. Lo mismo se aplicará, en circunstancias similares, a contratistas, expertos o asesores externos.

NORMAS ESPECÍFICAS SOBRE EL ACCESO A INFORMACIÓN TRÈS SECRET UE/EU TOP SECRET

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

6. Todas las personas que tengan que acceder a información TRÈS SECRET UE/EU TOP SECRET serán designadas por el jefe de su departamento y sus nombres constarán en el correspondiente registro TRÈS SECRET UE/EU TOP SECRET.

7. Antes de tener acceso a información TRÈS SECRET UE/EU TOP SECRET, todas las personas firmarán un certificado en el que constará que han recibido instrucciones relativas a los procedimientos de seguridad del Consejo y que son plenamente conscientes de su responsabilidad especial de proteger la información TRÈS SECRET UE/EU TOP SECRET, así como de las consecuencias previstas en la legislación 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.

8. En caso de que haya personas que accedan a información TRÈS SECRET UE/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.

9. Los nombres de todas las personas que dejen de desempeñar funciones para las cuales sea necesario el acceso a información TRÈS SECRET UE/EU TOP SECRET se eliminarán de la lista TRÈS SECRET UE/EU TOP SECRET. Además, se volverá a llamar la atención de dichas personas sobre su responsabilidad especial en relación con la protección de información TRÈS SECRET UE/EU TOP SECRET. También firmarán una declaración en la que constará que no utilizarán ni transmitirán información TRÈS SECRET UE/EU TOP SECRET que se encuentre en su poder.

NORMAS ESPECÍFICAS SOBRE EL ACCESO A INFORMACIÓN SECRET UE Y CONFIDENTIEL UE

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

11. Todas las personas que vayan a tener acceso a información SECRET UE o CONFIDENTIEL UE tendrán conocimiento de las correspondientes normas en materia de seguridad y deberán conocer las consecuencias de las negligencias.

12. En el caso de las personas que accedan a información SECRET UE o CONFIDENTIEL UE 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.

NORMAS ESPECÍFICAS SOBRE EL ACCESO A INFORMACIÓN RESTREINT UE

13. Se darán a conocer a las personas con acceso a información RESTREINT UE las presentes normas de seguridad, así como las consecuencias de las negligencias.

TRASLADOS

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

INSTRUCCIONES ESPECIALES

15. Las personas que tengan que tratar 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 la conversación indiscreta;

    b) las precauciones que han de tomar respecto de los medios informativos;

    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.

16. Todas las personas expuestas habitualmente a contacto frecuente con representantes de países cuyos servicios de inteligencia están interesados en la información y actividades clasificadas de la UE y de los Estados miembros asistirán a sesiones de información sobre las técnicas conocidas de los distintos servicios de inteligencia.

17. No existe en el Consejo una normativa de seguridad referente a los viajes privados que realiza el personal habilitado para acceder a información clasificada de la UE. No obstante, las autoridades de seguridad competentes darán a conocer a los funcionarios y otros agentes de su ámbito de responsabilidad las normas sobre viajes a las que puedan estar sujetos. Los encargados de la seguridad serán responsables de organizar reuniones de reciclaje para funcionarios en relación con las instrucciones especiales.

SECCIÓN VI

PROCEDIMIENTO DE HABILITACIÓN DE SEGURIDAD APLICABLE A LOS FUNCIONARIOS Y OTROS AGENTES DE LA SGC

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

2. Para acceder a la información clasificada TRÈS SECRET UE/EU TOP SECRET, SECRET UE y CONFIDENTIEL UE, las personas mencionadas en el apartado 1 deberán haber sido autorizadas con arreglo al procedimiento previsto en los apartados 4 y 5.

3. 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 los apartados 6 a 10.

4. Será responsable de la concesión de las autorizaciones previstas en los apartados 1, 2 y 3 la autoridad facultada para proceder a los nombramientos contemplada en el párrafo primero del artículo 2 del Estatuto de los funcionarios.

   La autoridad facultada para proceder a los nombramientos 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 los apartados 6 a 12.

5. 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 por la autoridad facultada para proceder a los nombramientos de acuerdo con el procedimiento previsto en el apartado 4.

   La autoridad facultada para proceder a los nombramientos podrá retirar la autorización si considera que hay motivos que lo justifican. Toda decisión de retirada de la autorización se notificará a la persona interesada, que podrá solicitar ser escuchada por la autoridad facultada para proceder a los nombramientos, y a la autoridad nacional competente.

6. El objetivo de la comprobación de seguridad será establecer que no hay objeciones a permitir a la persona de que se trate acceder a la información clasificada en poder del Consejo.

7. La comprobación de seguridad será realizada por las autoridades nacionales competentes del Estado miembro del que sea nacional la persona objeto de autorización con asistencia de la persona interesada y a petición de la autoridad facultada para proceder a los nombramientos. En caso de que la persona interesada resida en el territorio de otro Estado miembro, las autoridades nacionales interesadas podrán recurrir a la colaboración de las autoridades del Estado miembro de residencia.

8. En el marco del procedimiento de comprobación de seguridad, se podrá obligar a la persona interesada a rellenar una ficha personal de información.

9. La autoridad facultada para proceder a los nombramientos especificará en su solicitud el tipo y el nivel de información clasificada que se pondrá a disposición de la persona interesada, 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.

10. 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.

11. En caso de que las autoridades nacionales competentes de Estado miembro emitan un dictamen positivo, la autoridad facultada para proceder a los nombramientos podrá conceder la autorización a la persona interesada.

12. De emitirse un dictamen negativo, las autoridades nacionales competentes lo notificarán a la persona interesada, que podrá solicitar ser escuchada por la autoridad facultada para proceder a los nombramientos. Si lo considera necesario, la autoridad facultada para proceder a los nombramientos 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.

13. Todas las personas a las que se conceda autorización en el sentido de los apartados 4 y 5 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 harán constar que conocen las instrucciones y se comprometerán a obedecerlas.

14. La autoridad facultada para proceder a los nombramientos adoptará cualquier medida necesaria 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.

15. A título excepcional, en caso de que el servicio lo exija, la autoridad facultada para proceder a los nombramientos podrá, previa notificación a las autoridades nacionales competentes y siempre que éstas no respondan en el plazo de un mes, conceder una autorización temporal para un período que no superará los seis meses, en espera del resultado de la comprobación de seguridad prevista en el apartado 7.

16. Las autorizaciones provisionales y temporales concedidas de esta forma no darán acceso a información TRÈS SECRET UE/EU TOP SECRET; el acceso a esta información se limitará a los funcionarios que hayan superado efectivamente con éxito una comprobación de seguridad, con arreglo a lo previsto en el apartado 7. En espera del resultado de la comprobación de seguridad, los funcionarios para los que se ha solicitado una autorización de nivel TRÈS SECRET UE/EU TOP SECRET podrán ser autorizados con carácter temporal y provisional a acceder a información clasificada hasta el nivel SECRET UE inclusive.

SECCIÓN VII

ELABORACIÓN, DISTRIBUCIÓN, TRANSMISIÓN, ALMACENAMIENTO Y DESTRUCCIÓN DE MATERIAL CLASIFICADO DE LA UE

Índice

Página

Disposiciones generales

Capítulo I: Elaboración y distribución de documentos clasificados de la UE 23

Capítulo II: Transmisión de documentos clasificados de la UE 23

Capítulo III: Medios técnicos de transmisión eléctricos y otros 26

Capítulo IV: Copias adicionales y traducciones y extractos de documentos clasificados de la UE 26

Capítulo V: Inventarios y controles, almacenamiento y destrucción de documentos clasificados de la UE 26

Capítulo VI: Normas específicas aplicables a los documentos destinados al Consejo 28

Disposiciones generales

La presente sección precisa las medidas para la preparación, distribución, transmisión, almacenamiento y destrucción de documentos clasificados de la UE tal como se definen en la letra a) del apartado 3 de los Principios básicos y normas mínimas de seguridad establecidas en la parte I del presente anexo. Se utilizará como referencia para la adaptación de las medidas aplicables a otro material clasificado de la UE, con arreglo a su tipo y tratando los casos individualmente.

Capítulo I

Elaboración y distribución de documentos clasificados de la UE

ELABORACIÓN

1. Las clasificaciones y marcas de la UE se aplicarán según lo establecido en la sección II y figurarán en la parte central, superior e inferior, de cada página; todas las páginas irán numeradas. Todos los documentos clasificados de la UE llevarán número de referencia y fecha. En el caso de los documentos TRÈS SECRET UE/EU TOP SECRET y SECRET UE, 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. Todos los anexos y documentos adjuntos se indicarán en la primera página de los documentos clasificados CONFIDENTIEL UE y de nivel superior.

2. Los documentos clasificados CONFIDENTIEL UE y de nivel superior serán mecanografiados, traducidos, almacenados, fotocopiados, reproducidos magnéticamente o microfilmados únicamente por personas autorizadas a acceder a información clasificada de la UE como mínimo hasta el nivel de clasificación de seguridad correspondiente al documento de que se trate, a excepción del caso especial descrito en el apartado 27 de la presente sección.

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

DISTRIBUCIÓN

3. La información clasificada de la UE se distribuirá únicamente a las personas que tengan necesidad de conocerla y posean la debida habilitación de seguridad. La distribución inicial será indicada por el emisor.

4. Los documentos TRÈS SECRET UE/EU TOP SECRET se distribuirán mediante registros TRÈS SECRET UE/EU TOP SECRET (véase la sección VIII). En el caso de los mensajes TRÈS SECRET UE/EU TOP SECRET, el registro competente podrá autorizar al jefe del centro de comunicaciones a producir el número de copias indicado en la lista de destinatarios.

5. Cuando las circunstancias lo justifiquen, los documentos clasificados SECRET UE y de nivel inferior podrán ser distribuidos a su vez por los destinatarios originales a otros destinatarios. No obstante, las autoridades emisoras podrán hacer constar cualquier tipo de advertencia que deseen imponer. Cuando se impongan estas advertencias, los destinatarios podrán volver a distribuir los documentos únicamente con la autorización de las autoridades emisoras.

6. Cuando lleguen a la institución o salgan de ella, todos los documentos clasificados CONFIDENTIEL UE y de nivel superior se inscribirán en el registro de la institución. Se harán constar las características (referencia, fecha y, en su caso, número de copia) que permitan identificar los documentos en un registro o en soporte informatizado especialmente protegido.

Capítulo II

Transmisión de documentos clasificados de la UE

EMPAQUETADO

7. Los documentos clasificados CONFIDENTIEL UE y de nivel superior se transmitirán en sobres dobles opacos y de gran resistencia. El sobre interior irá marcado con la correspondiente clasificación de seguridad de la UE y, si es posible, con indicaciones completas de la denominación del cargo del destinatario y de su dirección.

8. Únicamente un controlador de registro, o su sustituto, podrán abrir el sobre interior y acusar recibo de los documentos adjuntos, salvo que el sobre vaya dirigido a una persona. En este caso, se hará constar en el registro correspondiente 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.

9. El sobre interior contendrá un impreso de recibo que no se clasificará y que indicará el número de referencia, la fecha y el número de copia del documento, pero nunca la materia que trata.

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

11. En el caso de los documentos clasificados CONFIDENTIEL UE y de nivel superior, los correos y mensajeros recibirán impresos de recibo contra los números de empaquetado.

TRANSMISIÓN DENTRO DE UN EDIFICIO O GRUPO DE EDIFICIOS

12. Dentro de un edificio o grupo de edificios determinado, los documentos clasificados podrán ser transportados en un sobre sellado con la única indicación del nombre del destinatario, a condición de que la persona que los transporte posea una habilitación equivalente al nivel de clasificación de los documentos.

TRANSMISIÓN DE DOCUMENTOS DE LA UE DENTRO DE UN PAÍS

13. Dentro de un país, los documentos TRÈS SECRET UE/EU TOP SECRET deben ser enviados únicamente a través de un servicio de mensajería oficial o por personas autorizadas para acceder a información TRÈS SECRET UE/EU TOP SECRET.

14. Siempre que se recurra a un servicio de mensajería para la transmisión de un documento TRÈS SECRET UE/EU TOP SECRET fuera de los límites físicos de un edificio o grupo de edificios, se aplicarán las disposiciones en materia de empaquetado 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 TRÈS SECRET UE/EU TOP SECRET permanezcan en todo momento bajo la supervisión directa de un funcionario responsable.

15. Excepcionalmente, funcionarios que no sean mensajeros podrán llevar documentos TRÈS SECRET UE/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 está autorizado para acceder a los citados documentos TRÈS SECRET UE/EU TOP SECRET;

    b) el modo de transporte cumple las normas nacionales en materia de transmisión de documentos nacionales de clasificación equivalente a TRÈS SECRET/TOP SECRET;

    c) el funcionario no descuida los documentos TRÈS SECRET UE/EU TOP SECRET en ningún momento;

    d) se dispone que en el registro TRÈS SECRET UE/EU TOP SECRET en que se conservan los documentos figura una lista de los documentos así transportados, que se registran en un diario y se controlan a su vuelta.

16. Dentro de un país dado, los documentos SECRET UE y CONFIDENTIEL UE 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.

17. Cada Estado miembro u organismo descentralizado de la UE dictará instrucciones relativas al 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 IV;

    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.

TRANSMISIÓN DE UN ESTADO MIEMBRO A OTRO

18. El material clasificado CONFIDENTIEL UE y de nivel superior deberá ser expedido de un Estado miembro a otro a través de servicios de correo diplomáticos o militares.

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

20. Las ANS podrán 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. Cada Estado miembro dictará instrucciones relativas al transporte personal internacional de material clasificado hasta el nivel SECRET UE inclusive por personas que no sean correos diplomáticos o militares. Dichas instrucciones deberán exigir lo siguiente:

a) el portador deberá poseer una autorización adecuada expedida por los Estados miembros;

b) se conservará un diario de los documentos transportados 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 de la UE que le 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 normas;

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 IV;

h) el material nunca podrá quedar descuidado en vehículos públicos o privados, o en lugares como restaurantes u hoteles. No 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.).

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

TRANSMISIÓN DE DOCUMENTOS RESTREINT UE

21. No se dispondrán medidas especiales para el envío de documentos RESTREINT UE, salvo las destinadas a garantizar que dichos documentos no caigan en manos de personas no autorizadas.

SEGURIDAD DEL PERSONAL DE CORREO

22. Todos los correos y mensajeros utilizados para llevar documentos SECRET UE y CONFIDENTIEL UE habrán de tener la debida habilitación de seguridad.

Capítulo III

Medios técnicos de transmisión eléctricos y otros

23. Las medidas de seguridad de las comunicaciones estarán concebidas para garantizar la transmisión segura de información clasificada de la UE. La sección XI recoge las normas detalladas aplicables a la transmisión de dicha información clasificada de la UE.

24. Únicamente los centros y redes o terminales y sistemas de comunicación acreditados podrán transmitir información clasificada CONFIDENTIEL UE y SECRET UE.

Capítulo IV

Copias adicionales y traducciones y extractos de documentos clasificados de la UE

25. Sólo el emisor podrá autorizar la copia o traducción de documentos TRÈS SECRET UE/EU TOP SECRET.

26. Si personas sin habilitación TRÈS SECRET UE/EU TOP SECRET necesitan información que, a pesar de figurar en un documento TRÈS SECRET UE/EU TOP SECRET, no tiene dicha clasificación, el jefe del registro TRÈS SECRET UE/EU TOP SECRET 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.

27. Los documentos clasificados SECRET UE o de nivel inferior podrán ser reproducidos y traducidos por el destinatario, dentro del marco de las normas de seguridad nacionales 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 subsiguientes. Los organismos descentralizados de la UE cumplirán las presentes normas de seguridad.

Capítulo V

Inventarios y controles, almacenamiento y destrucción de documentos clasificados de la UE

INVENTARIOS Y CONTROLES

28. Con periodicidad anual, cada registro TRÈS SECRET UE/EU TOP SECRET a que se hace referencia en la sección VIII llevará a cabo un inventario detallado de los documentos TRÈS SECRET UE/EU TOP SECRET con arreglo a las normas de los apartados 9 a 11 de la sección VIII. Los documentos clasificados de la UE de nivel inferior a TRÈS SECRET UE/EU TOP SECRET estarán sujetos a controles internos con arreglo a directrices nacionales y, en el caso de la SGC o de los organismos descentralizados de la UE, con arreglo a las instrucciones del Secretario General/Alto Representante.

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.

ALMACENAMIENTO DE INFORMACIÓN CLASIFICADA DE LA UE EN ARCHIVOS

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

a) el proceso de microfilmado o almacenamiento sea llevado a cabo por personal con habilitación vigente para el correspondiente nivel de clasificación;

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

c) el emisor sea informado sobre el microfilmado o almacenamiento de todo documento TRÈS SECRET UE/EU TOP SECRET;

d) los carretes de fotos, y otro tipo de soporte, contengan sólo documentos de la misma clasificación TRÈS SECRET UE/EU TOP SECRET, SECRET UE o CONFIDENTIEL UE;

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

f) los documentos originales que hayan sido microfilmados o almacenados se destruyan con arreglo a las normas establecidas en los apartados 31 a 36.

30. Estas normas se aplicarán también a cualquier otra forma de almacenamiento autorizada por la ANS, como los medios electromagnéticos o discos ópticos.

DESTRUCCIÓN SISTEMÁTICA DE DOCUMENTOS CLASIFICADOS DE LA UE

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

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

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

c) Los documentos TRÈS SECRET UE/EU TOP SECRET, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos TRÈS SECRET UE/EU TOP SECRET, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos bajo la supervisión de un funcionario TRÈS SECRET UE/EU TOP SECRET; la destrucción se hará quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles.

32. Los documentos SECRET UE serán destruidos por el registro responsable de dichos documentos, bajo la supervisión de una persona con habilitación de seguridad, utilizando uno de los procesos indicados en la letra c) del apartado 31. Los documentos SECRET UE que sean destruidos se incluirán en certificados de destrucción firmados que se guardarán en el registro, junto con los impresos de distribución, durante al menos tres años.

33. Los documentos CONFIDENTIEL UE serán destruidos por el registro responsable de dichos documentos, bajo la supervisión de una persona con habilitación de seguridad, utilizando uno de los procesos indicados en la letra c) del apartado 31. Se guardará constancia de su destrucción con arreglo a la normativa nacional y, en el caso de la SGC o de los organismos descentralizados de la UE, con arreglo a las instrucciones del Secretario General/Alto Representante.

34. Los documentos RESTREINT UE serán destruidos por el registro responsable de dichos documentos o por el usuario, con arreglo a la normativa nacional y, en el caso de la SGC o de los organismos descentralizados de la UE, con arreglo a las instrucciones del Secretario General/Alto Representante.

DESTRUCCIÓN EN EMERGENCIAS

35. La SGC, los Estados miembros y los organismos descentralizados de la UE prepararán planes basados en las condiciones locales para salvaguardar el material clasificado de la UE en una crisis y que incluyan, si fuera necesario, planes de destrucción y evacuación de emergencia; promulgarán, en sus respectivas organizaciones, las instrucciones que se estimen necesarias para impedir que la información clasificada de la UE caiga en manos de personas no autorizadas.

36. Las disposiciones para la salvaguardia o la destrucción de material SECRET UE y CONFIDENTIEL UE en una crisis no afectarán en ningún caso a la salvaguardia o destrucción de material TRÈS SECRET UE/EU TOP SECRET, incluido el equipo de mensajes cifrados, cuyo tratamiento debe tener prioridad sobre todas las demás tareas. Las medidas que deban adoptarse para la salvaguardia y destrucción del equipo de mensajes cifrados en una emergencia figurarán en instrucciones específicas.

Capítulo VI

Normas específicas aplicables a los documentos destinados al Consejo

37. Dentro de la SGC, una «Oficina de Información Clasificada» controlará la información clasificada SECRET UE o CONFIDENTIEL UE contenida en los documentos del Consejo.

Bajo la autoridad del Director General de Personal y de la Administración, dicha Oficina:

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

b) actualizará el registro de información clasificada;

c) periódicamente se interrogará sobre la necesidad de mantener la clasificación de la información;

d) establecerá, en colaboración con la Oficina de Seguridad, las disposiciones prácticas para la clasificación y desclasificación de información.

38. La Oficina de Información Clasificada mantendrá 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 departamento del autor;

e) el o los destinatarios, con el número de entrega;

f) el asunto;

g) el número;

h) el número de copias distribuidas;

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

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

39. Las normas generales establecidas en los capítulos I a V de la presente sección se aplicarán a la Oficina de Información Clasificada de la SGC, a no ser que se modifiquen por las normas específicas establecidas en el presente capítulo.

SECCIÓN VIII

REGISTROS TRÈS SECRET UE/EU TOP SECRET

1. El objetivo de los registros TRÈS SECRET UE/EU TOP SECRET es garantizar el almacenamiento, tratamiento y distribución de documentos TRÈS SECRET UE/EU TOP SECRET con arreglo a las presentes normas de seguridad. El jefe del registro TRÈS SECRET UE/EU TOP SECRET, respectivamente en cada Estado miembro, en la SGC y, cuando proceda, en los organismos descentralizados de la UE, será el controlador TRÈS SECRET UE/EU TOP SECRET.

2. Los registros centrales actuarán como la principal autoridad receptora y emisora en los Estados miembros, en la SGC y en los organismos descentralizados de la UE en los que se hayan establecido dichos registros, así como, cuando proceda, en otras instituciones de la UE, organizaciones internacionales y terceros Estados con los que el Consejo 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 TRÈS SECRET UE/EU TOP SECRET, que mantendrán datos actualizados sobre la circulación de cada documento a cargo del registro secundario.

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

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

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

REGISTROS CENTRALES TRÈS SECRET UE/EU TOP SECRET

7. En su calidad de controlador, el jefe de un registro central TRÈS SECRET UE/EU TOP SECRET será responsable de:

   a) transmitir los documentos TRÈS SECRET UE/EU TOP SECRET con arreglo a lo dispuesto en la sección VII;

   b) mantener una lista de todos sus registros secundarios dependientes TRÈS SECRET UE/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 TRÈS SECRET UE/EU TOP SECRET distribuidos por el registro central;

   d) mantener un registro de todos los documentos TRÈS SECRET UE/EU TOP SECRET guardados y distribuidos;

   e) mantener una lista actualizada de todos los registros centrales TRÈS SECRET UE/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 salvaguardia física de todos los documentos TRÈS SECRET UE/EU TOP SECRET en el registro con arreglo a las normas de la sección IV.

REGISTROS SECUNDARIOS TRÈS SECRET UE/EU TOP SECRET

8. En su calidad de controlador, el jefe de un registro secundario TRÈS SECRET UE/EU TOP SECRET será responsable de:

   a) transmitir los documentos TRÈS SECRET UE/EU TOP SECRET con arreglo a lo dispuesto en la sección VII y en los apartados 5 y 6 de la sección VIII;

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

c) distribuir los documentos TRÈS SECRET UE/EU TOP SECRET con arreglo a las instrucciones del emisor o según la necesidad de conocer que presente cada uno de ellos, comprobando en primer lugar que el destinatario tiene la habilitación de seguridad exigida;

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

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

f) velar por la salvaguardia física de todos los documentos TRÈS SECRET UE/EU TOP SECRET en el registro secundario con arreglo a las normas de la sección IV.

INVENTARIOS

9. Cada doce meses, cada registro TRÈS SECRET UE/EU TOP SECRET llevará a cabo un inventario detallado de todos los documentos TRÈS SECRET UE/EU TOP SECRET de los que ha de responder. Se considerará que se ha respondido de un documento si el registro cuenta físicamente con el documento, o guarda un recibo del registro TRÈS SECRET UE/EU TOP SECRET al que el documento ha sido transmitido, un certificado de destrucción del documento o una instrucción de recalificación o desclasificación de dicho documento.

10. Los registros secundarios presentarán los resultados de su inventario anual al registro central ante el que responden, en una fecha especificada por este último.

11. Las ANS, así como aquellas instituciones de la UE, organizaciones internacionales y organismos descentralizados de la UE en los que se haya creado un registro TRÈS SECRET UE/EU TOP SECRET, presentarán al Secretario General/Alto Representante, antes del 1 de abril de cada año, los resultados de sus inventarios anuales llevados a cabo en los registros centrales TRÈS SECRET UE/EU TOP SECRET.

SECCIÓN IX

MEDIDAS DE SEGURIDAD QUE DEBERÁN APLICARSE CON MOTIVO DE LA CELEBRACIÓN DE REUNIONES ESPECÍFICAS, FUERA DE LOS LOCALES DEL CONSEJO, QUE SE REFIERAN A ASUNTOS MUY SENSIBLES

GENERAL

1. Cuando reuniones del Consejo Europeo, del Consejo, de nivel ministerial u otras reuniones importantes se celebren fuera de los locales del Consejo en Bruselas y Luxemburgo, y cuando esté justificado por los requisitos específicos de seguridad relativos a los temas o a la información de que se trate, deberán adoptarse las medidas de seguridad descritas a continuación. Estas medidas afectan únicamente a la protección de información clasificada de la UE; podrá ser necesario prever otras medidas de seguridad.

RESPONSABILIDADES

Estados miembros de acogida

2. El Estado miembro en cuyo territorio se celebre la reunión (el Estado miembro de acogida) será responsable, en cooperación con la Oficina de Seguridad de la SGC, de la seguridad de las reuniones del Consejo Europeo, del Consejo, de nivel ministerial o de otras reuniones importantes, así como de la seguridad física de los delegados principales 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 del Consejo para la recepción y transmisión de mensajes clasificados de la UE. El Estado miembro de acogida proporcionará también acceso a sistemas de telefonía seguros si así se solicita.

Estados miembros

3. Las autoridades de los Estados miembros harán todo lo necesario para garantizar que:

a) se proporciona a sus delegados nacionales certificados de habilitación de seguridad adecuados, si fuese necesario mediante señales o por fax, ya sea directamente al agente de seguridad de la reunión, ya sea a través de la Oficina de Seguridad de la SGC;

b) cualquier amenaza concreta se comunica a las autoridades del Estado miembro de acogida y, cuando proceda, a la Oficina de Seguridad de la SGC de forma que puedan tomarse las medidas necesarias.

Agente de seguridad de la reunión

4. Deberá nombrarse un agente de seguridad que será responsable, en general, de la preparación y del control de las medidas generales de seguridad interna y de la coordinación con las otras autoridades de seguridad afectadas. Las medidas adoptadas por dicho agente se referirán en general a:

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

ii) 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;

iii) una coordinación constante con las autoridades competentes del Estado miembro de acogida y con la Oficina de Seguridad de la SGC;

b) 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.

Oficina de Seguridad de la SGC

5. La Oficina de Seguridad de la SGC deberá actuar como órgano consultor de seguridad para la preparación de la reunión; deberá estar representada *in situ* para ayudar y aconsejar al agente de seguridad de la reunión y a las delegaciones si fuere necesario.

6. Cada una de las delegaciones de la reunión deberá designar un agente de seguridad que será responsable de los asuntos de seguridad en su delegación y de mantener contactos con el agente de seguridad de la reunión, así como con el representante de la Oficina de Seguridad de la SGC, si fuere necesario.

MEDIDAS DE SEGURIDAD

Zonas de seguridad

7. 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 SGC 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 conferencia y las cabinas de sonido y de interpretación;

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

Pases

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

9. Las instrucciones de seguridad para 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.

10. Aparte de los participantes con tarjeta, deberá reducirse al máximo el número de personas que pueden entrar en el lugar de la reunión. Las delegaciones nacionales que deseen recibir visitas durante la reunión deberán notificarlo al agente de seguridad de la reunión. 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.

Control de los equipos de fotografía y sonido

11. 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 agente de seguridad de la reunión.

Control de maletines, ordenadores portátiles y paquetes

12. Las personas que detenten un pase con acceso a una zona de seguridad podrán normalmente llevar sus maletines y ordenadores portátiles (sólo con alimentación independiente) sin que se efectúe control alguno. Los paquetes dirigidos a las delegaciones 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 agente de seguridad de la reunión lo considera necesario, podrán establecerse medidas más severas de inspección de maletines y paquetes.

Seguridad técnica

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

Documentos de las delegaciones

14. Las delegaciones serán responsables de llevar los documentos clasificados de la UE tanto a la entrada como a la salida de las reuniones. También deberán ser responsables del control y de la seguridad de los mismos mientras los utilicen en los lugares destinados a ello. Podrán solicitar ayuda del Estado miembro de acogida para llevar los documentos clasificados a la entrada y a la salida de la reunión.

Custodia segura de los documentos

15. Si la SGC, la Comisión o las delegaciones no pudieran guardar sus documentos clasificados de conformidad con las normas establecidas, podrán introducirlos en sobres sellados y entregarlos contra recibo al agente de seguridad de la reunión, para que éste pueda guardarlos según las normas establecidas.

Control de los despachos

16. El agente de seguridad de la reunión dispondrá que al término de cada jornada de trabajo se realice una inspección de los despachos de la SGC y de las delegaciones para garantizar que todos los documentos clasificados de la UE están seguros; si no fuera así, tomará las medidas oportunas.

Destrucción de los restos de documentos clasificados de la UE

17. Todos los restos de documentos deberán considerarse material clasificado de la UE. Deberán entregarse papeleras y bolsas a la SGC y a las delegaciones para que recojan los papeles. La SGC y las delegaciones deberán entregar los papeles al agente de seguridad de la reunión antes de abandonar los lugares que les fueron asignados. El agente ordenará su destrucción según las normas.

18. Al final de la reunión, todos los documentos que la SGC o las delegaciones ya no deseen serán tratados como restos de documentos. Antes de retirar las medidas de seguridad decretadas para la reunión se llevará a cabo un registro exhaustivo de los locales utilizados por la SGC y por las delegaciones. En la medida de lo posible, los documentos que se entregaron contra recibo serán destruidos de conformidad con lo dispuesto en la sección VII.

SECCIÓN X

QUEBRANTAMIENTOS DE LA SEGURIDAD Y PUESTA EN PELIGRO DE INFORMACIÓN CLASIFICADA DE LA UE

1. Un quebrantamiento de la seguridad es un acto u omisión contrario a una norma de seguridad del Consejo o nacional que pueda poner en peligro información clasificada de la UE.

2. La puesta en peligro de información clasificada de la UE ocurre cuando ésta cae enteramente o en parte en manos de personas no autorizadas, es decir, que ni tienen la autorización de seguridad ni la necesidad de conocer pertinentes, o cuando existe la probabilidad de que se haya producido este hecho.

3. La información clasificada de la UE puede ponerse en peligro por descuido, negligencia o indiscreción, o bien debido a actividades de servicios de espionaje cuyo objetivo es la UE o sus Estados miembros, por cuanto se refiere a la información clasificada y a las actividades de la UE, o bien por organizaciones de carácter subversivo.

4. Es importante que todas las personas que traten información clasificada de la UE hayan recibido instrucciones detalladas sobre los procedimientos de seguridad, los peligros de las conversaciones indiscretas y sus relaciones con los medios informativos. Esas personas deberían ser conscientes de la importancia de comunicar inmediatamente cualquier quebrantamiento de la seguridad que pudieran observar a la autoridad de seguridad del Estado miembro, de la institución o del organismo donde trabajen.

5. Cuando una autoridad de seguridad descubra o sea informada de un quebrantamiento de la seguridad de información clasificada de la UE, o de la desaparición de material clasificado de la UE, deberá tomar inmediatamente medidas para:

   a) aclarar los hechos;

   b) evaluar los daños causados y reducirlos al mínimo;

   c) impedir que los hechos se repitan;

   d) notificar a las autoridades competentes los efectos del quebrantamiento de la seguridad.

   En este contexto, deberán aportarse los siguientes datos:

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

   ii) breve descripción de las circunstancias en que se ha producido el quebrantamiento de la seguridad, con la fecha y el período en que pudo ponerse en peligro la información;

   iii) declaración sobre si se ha informado al emisor.

6. Cada autoridad de seguridad deberá, en cuanto se le notifique que puede haberse producido un quebrantamiento de la seguridad, informar inmediatamente del hecho mediante el siguiente procedimiento: el registro TRÈS SECRET UE/EU TOP SECRET deberá informar a la Oficina de Seguridad de la SGC a través de su registro central TRÈS SECRET UE/EU TOP SECRET; si la información clasificada de la UE hubiera sido puesta en peligro dentro de la jurisdicción de un Estado miembro, se informará de ello a la Oficina de Seguridad de la SGC, tal como se especifica en el apartado 5, a través de la ANS competente.

7. Sólo se deberá informar de los casos relativos a información clasificada RESTREINT UE cuando presenten características anómalas.

8. Cuando se le comunique un quebrantamiento de la seguridad, el Secretario General/Alto Representante:

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

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

   c) coordinará las investigaciones cuando intervenga en ellas más de una autoridad de seguridad;

d) obtendrá un informe sobre las circunstancias en que se produjo el quebrantamiento, la fecha o período en que pudo tener lugar y en que fue descubierto, 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.

9. La autoridad emisora deberá informar a los destinatarios y dar las instrucciones pertinentes.

10. 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. Dichas medidas no serán obstáculo para actuar ante los tribunales.

SECCIÓN XI

PROTECCIÓN DE LA INFORMACIÓN TRATADA EN LOS SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN Y DE COMUNICACIÓN

Índice

Página

Capítulo I Introducción 37

Capítulo II Definiciones 38

Capítulo III Competencias en materia de seguridad 41

Capítulo IV Medidas de seguridad de carácter no técnico 42

Capítulo V Medidas de seguridad de carácter técnico 43

Capítulo VI Seguridad durante el tratamiento 45

Capítulo VII Adquisición 45

Capítulo VIII Utilización temporal u ocasional 46

Capítulo I

Introducción

ASPECTOS DE CARÁCTER GENERAL

1. La política y los requisitos de seguridad expuestos en la presente sección se aplicarán a todos los sistemas y redes de comunicación (en lo sucesivo, «SISTEMAS») que traten información clasificada CONFIDENTIEL UE o de nivel superior.

2. Los SISTEMAS que traten información RESTREINT UE también necesitarán medidas de seguridad para proteger la confidencialidad de esa información. Todos los SISTEMAS necesitarán medidas de seguridad para proteger tanto su propia integridad y disponibilidad como la de la información que contienen. La Autoridad de Autorización de la Seguridad (AAS) designada determinará las medidas de seguridad que se aplicarán a esos sistemas y que serán proporcionales a los riesgos previstos y conformes a lo establecido en las presentes normas de seguridad.

3. La protección de los sistemas sensores que contengan SISTEMAS de TI integrados se determinará y definirá en el contexto general de los sistemas a los que pertenezcan, utilizando en lo posible las disposiciones aplicables de la presente sección.

AMENAZAS Y VULNERABILIDAD DE LOS SISTEMAS

4. En términos generales, 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 vulnerabilidad puede ser por omisión o deberse a alguna deficiencia en el grado, el alcance o la coherencia del control; puede ser de carácter técnico, procesal u operativo.

5. 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 numerosos riesgos. Entre ellos 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 equipo, complejo y a menudo frágil, resulta costoso y suele ser difícil de reparar o de sustituir rápidamente. Tales SISTEMAS son pues muy atractivos como objetivos de las operaciones de espionaje y sabotaje, particularmente cuando se piensa que las medidas de seguridad no son eficaces.

MEDIDAS DE SEGURIDAD

6. El principal objetivo de las medidas de seguridad expuestas en esta sección es prestar protección frente a la divulgación no autorizada de información (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, es necesario definir unas normas adecuadas de seguridad convencional junto con los procedimientos especiales de seguridad pertinentes y las técnicas particularmente ideadas para cada SISTEMA.

7. Se definirá y aplicará un conjunto equilibrado de medidas de seguridad para crear un entorno seguro en el que opere el SISTEMA. Los ámbitos de aplicación de esas medidas se refieren a los elementos físicos, al personal, a los procedimientos no técnicos y a los procedimientos operativos informáticos y de comunicaciones.

8. Las medidas de seguridad informática (características de seguridad del soporte material y de los programas) deberán respetar el principio de necesidad de conocer e impedir o detectar la divulgación no autorizada de información. Durante el proceso de definición de los requisitos de seguridad se irá determinando en qué medida las medidas de seguridad informática son fiables. El proceso de autorización deberá comprobar la existencia de un nivel adecuado de seguridad que justifique la fiabilidad de las medidas de seguridad informática.

ENUNCIACIÓN DE LOS REQUISITOS ESPECÍFICOS DE SEGURIDAD DEL SISTEMA (RESS)

9. La Autoridad Operativa del Sistema de Tecnología de la Información (AOSTI) deberá enunciar los requisitos específicos de seguridad del SISTEMA (RESS) para todos los SISTEMAS que traten información clasificada CONFIDENTIEL UE o de nivel superior, en colaboración con el personal del proyecto y con la Autoridad INFOSEC y, si ha lugar, con su contribución y asistencia; los RESS deberán ser aprobados por la AAS. Será igualmente necesario enunciar los RESS siempre que la AAS considere de capital importancia la disponibilidad e integridad de la información clasificada RESTREINT UE o de información no clasificada.

10. Conviene enunciar los RESS desde el primer momento de concepción del proyecto y desarrollarlos y perfeccionarlos a medida que el proyecto avance, de forma que desempeñen diversas funciones en las diferentes fases del ciclo vital del proyecto y del SISTEMA.

11. Los RESS constituirán el acuerdo vinculante entre la AOSTI y la AAS ante la cual vaya a autorizarse el SISTEMA.

12. Los RESS constituyen 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 del Consejo, 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 RESS 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 RESS constituyen una verdadera enumeración de los parámetros de seguridad del SISTEMA.

MODOS OPERATIVOS DE SEGURIDAD

13. Todos los SISEMAS que traten información clasificada CONFIDENTIEL UE o de nivel superior podrán estar 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.

Capítulo II

Definiciones

MARCADOS ADICIONALES

14. Se aplicarán marcados adicionales, tales como CRYPTO o cualquier otra designación especial de tratamiento reconocida a escala de la UE, cuando se dé una necesidad de distribución limitada y de tratamiento especial además del designado por la clasificación de seguridad.

15. 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.

16. 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.

17. 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.

18. Por SEGURIDAD INFORMÁTICA (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 las de seguridad de ordenadores, de divulgación, de emisión y de carácter criptográfico, así como la detección, documentación y respuesta a las amenazas contra la información y los SISTEMAS.

19. 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 proteger dicho sistema frente a las divulgaciones, manipulaciones, modificaciones o supresiones no autorizadas de información, o para impedir la denegación de servicio.

20. Por PRODUCTO DE SEGURIDAD INFORMÁTICA se entenderá un elemento informático genérico destinado a su incorporación a un sistema informático con objeto de mejorar o garantizar la confidencialidad, la integridad o la disponibilidad de la información tratada.

21. 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 dichas telecomunicaciones.

Nota:

Dichas medidas incluyen la seguridad de la criptografía, de la transmisión y de la emisión; y también la seguridad de los procedimientos, de los elementos físicos, del personal, de los documentos y del ordenador.

22. 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.

23. Por CERTIFICACIÓN se entenderá la emisión de una declaración formal basada en un examen independiente acerca de la manera en que se ha llevado a cabo la evaluación y de los resultados de ésta, así como de la medida en que un SISTEMA cumple la exigencia de seguridad o un producto de seguridad informática cumple los requisitos de seguridad previamente establecidos.

24. 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 después de la 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 el RESS 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 propone;

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 (SECOP), 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 las medidas de seguridad;

e) el plan de las pruebas iniciales y sucesivas de la seguridad del sistema o de la red, la evaluación y la certificación;

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

25. Por SISTEMA DE TI se entenderá un conjunto de equipo, 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 una única AOSTI.

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

26. Las MEDIDAS DE SEGURIDAD DE UN SISTEMA DE TI comprenden todas las funciones y características de soporte material, microprogramas y programas informáticos; procedimientos operativos, procedimientos de responsabilidad y controles de acceso, zona de TI, 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 TI.

27. Por RED DE TI se entenderá la organización, geográficamente dispersa, de sistemas de TI interconectados para el intercambio de datos, incluidos los componentes de los sistemas de TI interconectados y su interfaz con las redes de datos o redes de comunicación de apoyo.

Notas:

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

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

28. Los DISPOSITIVOS DE SEGURIDAD DE UNA RED DE TI comprenden los dispositivos de seguridad de cada sistema de TI 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).

29. Por ZONA DE TI 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 TI.

30. 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 TI.

31. Por contramedidas TEMPEST se entenderán 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.

Capítulo III

Competencias en materia de seguridad

ASPECTOS GENERALES

32. Las competencias del Comité de Seguridad, definidas en el apartado 4 de la sección I, incluyen cuestiones de INFOSEC. El Comité de Seguridad organizará sus actividades de manera tal que pueda facilitar un asesoramiento experto en las cuestiones antes mencionadas.

33. En caso de que surjan problemas relativos a la seguridad (incidentes, quebrantamientos, etc.), la autoridad nacional competente o la Oficina de Seguridad de la GSC deberá tomar medidas inmediatas. Todos los problemas deberán someterse a la Oficina de Seguridad de la GSC.

34. El Secretario General/Alto Representante o, en su caso, el jefe de un organismo descentralizado de la UE, deberá establecer una oficina INFOSEC para facilitar directrices a la autoridad de seguridad en lo que se refiere a la aplicación y el control de características específicas de seguridad proyectadas como parte de los SISTEMAS.

AUTORIDAD DE ACREDITACIÓN EN MATERIA DE SEGURIDAD (AAS)

35. La AAS puede ser:

— una ANS;

— la autoridad designada por el Secretario General/Alto Representante;

— la autoridad de seguridad de un organismo descentralizado de la UE;

— sus representantes, delegados o nombrados por ellos, en función del SISTEMA que deba acreditarse.

36. La AAS se encargará de garantizar la conformidad de los SISTEMAS con la política de seguridad del Consejo. 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. En lo que se refiere a la SGC y, si ha lugar, a los organismos descentralizados de la UE, la AAS tendrá la competencia de la seguridad en nombre del Secretario General/Alto Representante o de los jefes de los organismos descentralizados.

La jurisdicción de la AAS de la SGC incluirá todos los SISTEMAS operativos en los locales de las SGC. Los SISTEMAS y componentes de SISTEMAS operativos en un Estado miembro permanecerán bajo la jurisdicción de dicho Estado miembro. Cuando diversos componentes de un SISTEMA recaigan en la jurisdicción de la AAS de la SGC y de otras AAS, todas las partes designarán un comité común de acreditación bajo la coordinación de la AAS de la SGC.

AUTORIDAD INFOSEC

37. La Autoridad INFOSEC se encargará de las actividades de la oficina INFOSEC. En lo que se refiere a la SGC y, si ha lugar, a los organismos descentralizados de la UE, la Autoridad INFOSEC se encargará de las siguientes actividades:

— facilitar asesoramiento técnico y asistencia a la AAS;

— prestar asistencia en el desarrollo de los RESS;

— revisar los RESS 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 AAS 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.

AUTORIDAD OPERATIVA DEL SISTEMA DE TECNOLOGÍA DE LA INFORMACIÓN (AOSTI)

38. La Autoridad INFOSEC delegará cuanto antes la responsabilidad para la aplicación y el manejo de los controles y de las características específicas de seguridad del SISTEMA en la AOSTI. Dicha responsabilidad se prolongará durante todo el ciclo vital del SISTEMA, desde la fase de concepción del proyecto hasta su descarte definitivo.

39. La AOSTI se encargará de todas las medidas de seguridad proyectadas como parte del SISTEMA global. Dicha responsabilidad incluirá la preparación de los SECOP. La AOSTI especificará las normas y prácticas de seguridad que deba cumplir el suministrador del SISTEMA.

40. Si procede, la AOSTI podrá delegar una parte de sus responsabilidades, por ejemplo, en el agente de seguridad INFOSEC y en el agente de seguridad INFOSEC del emplazamiento. Una sola persona podrá realizar las diversas funciones de INFOSEC.

USUARIOS

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

FORMACIÓN INFOSEC

42. Se ofrecerá formación e información INFOSEC, a varios niveles y para diversos miembros del personal, según convenga, en la GSC, los organismos descentralizados de la UE o los ministerios de los Estados miembros.

Capítulo IV

Medidas de seguridad de carácter no técnico

SEGURIDAD DEL PERSONAL

43. 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 del Consejo.

44. La AAS designará todos los puestos sensibles y definirá el nivel de autorización y supervisión exigido a todo el personal que los ocupe.

45. 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. Esta medida tiene por objeto que no se pueda alterar ni degradar intencionadamente el sistema sin la participación de dos o más personas.

SEGURIDAD FÍSICA

46. Las zonas de TI y las zonas de terminales o puestos de trabajo remotos (según la definición que consta en los apartados 29 y 30) en las que una información clasificada CONFIDENTIEL UE y de nivel superior se trate con medios de TI, 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, o de la categoría nacional equivalente, según convenga.

47. Las zonas de TI 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.

CONTROL DE ACCESO A UN SISTEMA

48. 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.

49. Cuando ya no se utilice para dicho fin, la información y el material de control de acceso deberán ser destruidos de conformidad con los apartados 61 a 63.

Capítulo V

Medidas de seguridad de carácter técnico

SEGURIDAD DE LA INFORMACIÓN

50. El emisor 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 sea 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.

51. Una organización 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.

52. 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.

53. 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.

54. 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.

55. 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 con arreglo a un procedimiento aprobado por la SGC o a escala nacional (véanse apartados 61 a 63).

CONTROL Y FIABILIDAD DE LA INFORMACIÓN

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

57. Los productos clasificados de la UE que se mantengan en la zona de TI 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.

58. Cuando un SISTEMA genere un producto que trate información clasificada de la UE y se transmita de una zona de TI a una zona de terminales o puestos de trabajo remotos, se crearán procedimientos, aprobados por la AAS, para controlar el producto remoto. Para la clasificación SECRET UE y de nivel superior, dichos procedimientos incluirán instrucciones específicas respecto de la fiabilidad de la información.

TRATAMIENTO Y CONTROL DE LOS SOPORTES INFORMÁTICOS REMOVIBLES

59. Todos los soportes informáticos removibles clasificados CONFIDENTIEL UE 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.

60. 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.

DESCLASIFICACIÓN Y DESTRUCCIÓN DE SOPORTES INFORMÁTICOS

61. Los soportes informáticos utilizados para registrar información clasificada de la UE podrán ser recalificados o desclasificados siempre y cuando se les apliquen procedimientos aprobados por la SGC o a nivel nacional.

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

63. Los soportes informáticos que no puedan desclasificarse ni reutilizarse se destruirán con arreglo a un procedimiento aprobado por la SGC o a nivel nacional.

SEGURIDAD DE LAS COMUNICACIONES

64. 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 AAS 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.

65. Cuando sea preciso usar métodos criptográficos para proteger la confidencialidad, integridad y disponibilidad, dichos métodos y los productos asociados serán específicamente aprobados a tal fin por la AAS.

66. Durante la transmisión, la confidencialidad de la información clasificada SECRET UE o de nivel superior estará protegida por métodos o productos criptográficos aprobados por el Consejo a recomendación del Comité de Seguridad del Consejo. Durante la transmisión, la confidencialidad de la información clasificada CONFIDENTIEL UE o RESTREINT UE estará protegida por métodos o productos criptográficos aprobados ya sea por el Secretario General/Alto Representante a recomendación del Comité de Seguridad del Consejo, ya sea por un Estado miembro.

67. Se establecerán normas detalladas aplicables a la transmisión de información clasificada de la UE en las instrucciones específicas de seguridad aprobadas por el Consejo a recomendación del Comité de Seguridad del Consejo.

68. En circunstancias operativas excepcionales, la información clasificada RESTREINT UE, CONFIDENTIEL UE y SECRET UE podrán transmitirse en forma de texto claro siempre y cuando ello se autorice expresamente en cada ocasión. 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.

69. 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 AAS.

SEGURIDAD EN MATERIA DE INSTALACIÓN Y RADIACIONES

70. 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.

71. Todo el equipo deberá instalarse de conformidad con las disposiciones vigentes de seguridad del Consejo.

72. Los SISTEMAS que traten información clasificada CONFIDENTIEL UE o de nivel superior estarán protegidos de tal modo que su seguridad no pueda estar amenazada por radiaciones comprometedoras, cuyo examen y prevención se designarán con el término TEMPEST.

73. Las contramedidas TEMPEST para las instalaciones de la SGC y de los organismos descentralizados de la UE serán estudiadas y aprobadas por una autoridad TEMPEST designada por la autoridad de seguridad de la SGC. La autoridad de aprobación competente para las instalaciones nacionales que traten información clasificada de la UE será la autoridad nacional de aprobación TEMPEST reconocida.

Capitulo VI

Seguridad durante el tratamiento

PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD (SECOP)

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

GESTIÓN DE LA PROTECCIÓN Y CONFIGURACIÓN DE LOS PROGRAMAS INFORMÁTICOS

75. 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 se comprobarán periódicamente para garantizar su integridad y correcto funcionamiento.

76. No se utilizarán versiones nuevas o modificadas de los programas informáticos para el tratamiento de la información clasificada de la UE hasta que no los haya comprobado la AOSTI.

CONTROL DE LA PRESENCIA DE PROGRAMAS INFORMÁTICOS MALINTENCIONADOS O DE VIRUS INFORMÁTICOS

77. Se llevarán a cabo controles de la presencia de programas informáticos malintencionados o de virus informáticos, de conformidad con los requisitos de la AAS.

78. Antes de su introducción en cualquier SISTEMA, todos los soportes informáticos que lleguen a la SGC, a los organismos descentralizados de la UE o a los Estados miembros deberán verificarse con objeto de detectar la presencia de cualquier programa informático malintencionado o virus informático.

MANTENIMIENTO

79. Los contratos y procedimientos para el mantenimiento, ya sea éste programado o realizado previa petición, de los SISTEMAS para los que se haya efectuado un RESS especificarán los requisitos y las disposiciones aplicables al personal de mantenimiento y al equipo correspondiente que entre en una zona de TI.

80. Los requisitos y procedimientos se indicarán con claridad, respectivamente, en el RESS y en los SECOP. 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 AAS.

Capítulo VII

Adquisición

81. Todo producto de seguridad que vaya a utilizarse con el SISTEMA y deba adquirirse deberá haberse 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 según criterios reconocidos a escala internacional (tales como los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, ISO 15408).

82. 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 AAS, y que dicha aprobación no siempre será posible.

ACREDITACIÓN

83. Antes de tratar información clasificada de la UE, todos los SISTEMAS para los que se necesite un RESS deberán ser acreditados por la AAS a tenor de la información contenida en el RESS, en los SECOP 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 al Consejo y a otras organizaciones, la SGC y las autoridades de seguridad pertinentes acordarán mutuamente la acreditación.

84. El proceso de acreditación podrá efectuarse con arreglo a una estrategia adecuada a un determinado SISTEMA y definida por la AAS.

EVALUACIÓN Y CERTIFICACIÓN

85. 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.

86. Los requisitos para la evaluación y certificación se incluirán en la planificación del sistema y se indicarán claramente en el RESS.

87. 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 de la AOSTI.

88. 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.

89. 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.

CONTROL SISTEMÁTICO DE LOS ELEMENTOS DE SEGURIDAD PARA UNA ACREDITACIÓN CONTINUA

90. La AOSTI deberá establecer procedimientos de control sistemático que garanticen que todos los dispositivos de seguridad del SISTEMA siguen siendo válidos.

91. Los tipos de modificación que requieran una nueva acreditación o la aprobación previa de la AAS deberán identificarse claramente y enunciarse en el RESS. Después de cualquier modificación, reparación o fallo que pueda haber afectado a los dispositivos de seguridad del SISTEMA, la AOSTI 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.

92. La AAS 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 TRÈS SECRET UE/EU TOP SECRET o con marcado complementario, las inspecciones se efectuarán al menos una vez al año.

Capítulo VIII

Utilización temporal u ocasional

SEGURIDAD DE LOS MICROORDENADORES Y DE LOS ORDENADORES PERSONALES (PC)

93. Los microordenadores y ordenadores personales (PC) 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 removibles.

94. 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).

UTILIZACIÓN DE EQUIPOS PRIVADOS PARA TRABAJOS OFICIALES DEL CONSEJO

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

96. 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 el permiso del jefe de la Oficina de Seguridad de la SGC, del ministerio de un Estado miembro o del correspondiente organismo descentralizado de la UE.

UTILIZACIÓN DE EQUIPO PERTENECIENTE A UN CONTRATISTA FACILITADO POR UN PAÍS PARA UN TRABAJO OFICIAL DEL CONSEJO

97. La utilización de equipo y de programas informáticos de TI pertenecientes a un contratista en una organización para prestar apoyo a los trabajos oficiales del Consejo podrá ser autorizada por el jefe de la Oficina de Seguridad de la SGC, del ministerio de un Estado miembro o del correspondiente organismo descentralizado de la UE. Asimismo podrá autorizarse la utilización, por los funcionarios de la SGC o de un organismo descentralizado de la UE, de equipo y programas informáticos de TI suministrados por los Estados miembros; en tal caso, el equipo de TI se someterá al control del inventario de la SGC adecuado. En ambos casos, si el equipo de TI sirve para tratar información clasificada de la UE, se consultará a la AAS pertinente con objeto de que se consideren y lleven a efecto debidamente los elementos de INFOSEC que sean aplicables a la utilización de ese equipo.

SECCIÓN XII

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

PRINCIPIOS QUE RIGEN LA COMUNICACIÓN DE INFORMACIÓN CLASIFICADA DE LA UE

1. La comunicación de información clasificada de la UE a terceros países u organizaciones internacionales será decidida por el Consejo a tenor:

   — del carácter y el contenido de dicha información;

   — de la necesidad de conocer que tenga el destinatario;

   — de la apreciación de las ventajas para la UE.

   Se solicitará la aprobación del Estado miembro emisor de la información clasificada de la UE que deba entregarse.

2. 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 Comité de Seguridad del Consejo facilitará al Consejo su dictamen técnico sobre este punto.

3. 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 el Consejo.

NIVELES

4. Una vez que el Consejo 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.

5. 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.

6. Cada nivel de cooperación determinará las normas de seguridad, reformuladas en cada caso según el dictamen técnico del Comité de Seguridad del Consejo, que se pedirá que los beneficiarios apliquen a la protección de la información clasificada que se les entregue. Dichos procedimientos y normas de seguridad se exponen en los Anexos 4, 5 y 6.

ACUERDOS

7. Una vez que el Consejo haya decidido que existe una necesidad permanente o a largo plazo de intercambiar información clasificada entre la UE 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.

8. 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 RESTREINT UE.

9. Los proyectos de acuerdo sobre procedimientos de seguridad o los memorandos de entendimiento serán aprobados por el Comité de Seguridad antes de someterlos al Consejo para que éste decida.

10. Las ANS facilitarán al Secretario General/Alto Representante toda la asistencia necesaria 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

Lista de Autoridades Nacionales de Seguridad

BÉLGICA

Ministère des Affaires Etrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Teléfono: 32-2-501 85 14
Fax: 32-2-501 80 58
Télex: 21376
Dirección telegráfica: Direction de Sécurité A01 — MINAFET

DINAMARCA

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Teléfono: 45 33 14 88 88
Fax: 45 38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø.
Teléfono: 45 33 32 55 66
Fax: 45 33 93 13 20

ALEMANIA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Teléfono: 49-30-39 81 15 28
Fax: 49-30-39 81 16 10

GRECIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετράωρο)
Φαξ: 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos — Athens
Greece
Teléfono: 00 30-1-655 22 03 (en horas de oficina)
00 30-1-655 22 05 (24 horas)
Fax: 00 30-1-642 69 40

ESPAÑA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
Teléfono: 34-91-372 57 07
Fax: 34-91-372 58 08
E-mail: nsa-sp@areatec.com

FRANCIA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Teléfono: 33-0-144 18 81 80
Fax: 33-0-144 18 82 00
Télex: SEGEDEFNAT 200019
Dirección telegráfica: SEGEDEFNAT PARIS

IRLANDA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Teléfono: 353-1-478 08 22
Fax: 353-1-478 14 84

ITALIA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Teléfono: 39-06-627 47 75
Fax: 39-06-614 33 97
Télex: 623876 AQUILA 1
Dirección telegráfica: ess: PCM-ANS-UCSI-ROMA

LUXEMBURGO

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L-1023 Luxembourg
Teléfono: 352-478 22 10 central
352-478 22 35 directo
Fax: 352-478 22 43
352-478 22 71
Télex: 3481 SERET LU
Dirección telegráfica: MIN D'ETAT — ANS

PAÍSES BAJOS

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Teléfono: 31-70-320 44 00
Fax: 31-70-320 07 33
Télex: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Teléfono: 31-70-318 70 60
Fax: 31-70-318 79 51

AUSTRIA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Teléfono: 43-1-531 15 34 64
Fax: 43-1-531 8 52 19

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Teléfono: 351-21-301 55 10
351-21-301 00 01, extensión 20 45 37
Fax: 351-21-302 03 50

FINLANDIA

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Teléfono: 358-9-13 41 53 38
Fax: 358-9-13 41 53 03

SUECIA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Teléfono: 46-8-405 54 44
Fax: 46-8-723 11 76

REINO UNIDO

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1 AH
Teléfono: 44-20-72 70 87 51
Fax: 44-20-76 30 14 28
Dirección telegráfica: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Apéndice 2

Comparación de las clasificaciones de seguridad nacionales

Clasificación UE	TRÈS SECRET UE/EU TOP SECRET (UE altamente secreto)	SECRET UE (UE secreto)	CONFIDENTIEL UE (UE confidencial)	RESTREINT UE (UE reservado)
Clasificación OTAN ([1])				
Clasificación UEO	Focal Top Secret	WEU Secret	WEU Confidential	WEU 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 ([2])- VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Grecia	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
España	Secreto	Reservado	Confidencial	Difusión limitada
Francia	Très Secret Défense ([3])	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	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 Unión Europea y la OTAN.
([2]) Alemania: VS = Verschlusssache.
([3]) Francia: La clasificación «Très Secret Défense», que se refiere a las prioridades del Gobierno, sólo puede cambiarse con la autorización del Primer Ministro.

Apéndice 3

Guía práctica de clasificación

Esta guía es indicativa y no debe interpretarse que modifica las disposiciones sustantivas expuestas en las secciones II y III.

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
TRÈS SECRET UE/ EU TOP SECRET (UE altamente secreto): 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 [SII§1].	Si existe la probabilidad de que la puesta en peligro de materiales marcados TRÈS SECRET UE/EU TOP SECRET: — amenace directamente la estabilidad interna de la UE o de alguno de sus Estados miembros o de países amigos; — cause un perjuicio excepcionalmente grave a las relaciones con gobiernos amigos; — ocasione directamente la pérdida generalizada de vidas humanas; — 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; — ocasione un grave daño a largo plazo a la economía de la UE o de los Estados miembros.	Estados miembros: personas debidamente autorizadas (emisores) [SIII§4]; SGC: personas debidamente autorizadas (emisores) [SIII§4]; Secretario General/Alto Representante y Secretario General Adjunto. Los emisores deberán especificar la fecha o plazo en que el contenido pueda ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años como mínimo, para comprobar si la clasificación original sigue siendo necesaria [SIII§10].	La clasificación TRÈS SECRET UE/EU TOP SECRET se aplicará a los documentos TRÈS SECRET UE/EU TOP SECRET y, cuando proceda, se pondrá la indicación ESDP (PESD), por medios mecánicos y a mano [SII§8]. Las clasificaciones de la UE figurarán en la parte central, superior e inferior, de cada página; todas las páginas irán numeradas. Todos los documentos 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 [SVII§1].	La desclasificación o recalificación depende únicamente del emisor o del Secretario General/Alto Representante, que informarán de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [SIII§9]. Los documentos TRÈS SECRET UE/EU TOP SECRET serán destruidos por el registro central o por el registro secundario encargado de su custodia. Los documentos destruidos serán enumerados en un certificado de destrucción, firmado por el controlador TRÈS SECRET UE/EU TOP SECRET y por el funcionario que haya presenciado la destrucción, que tendrá la habilitación TRÈS SECRET UE/EU TOP SECRET. En el libro de registro se hará un apunte al efecto. El registro guardará los certificados de destrucción, junto con los impresos de distribución, durante diez años [SVII§31].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [SVII§31]. Los documentos TRÈS SECRET UE/EU TOP SECRET, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos TRÈS SECRET UE/EU TOP SECRET, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos bajo la supervisión de un funcionario TRÈS SECRET UE/EU TOP SECRET; la destrucción se hará quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [SVII§31].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
SECRET UE (UE secreto): 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 [SII§2].	Si existe la probabilidad de que la puesta en peligro de materiales marcados SECRET UE: — 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; — ocasione 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 sumamente valiosas; — ocasione un considerable daño material a los intereses financieros, monetarios, económicos o comerciales de la UE o de uno de sus Estados miembros.	Estados miembros: personas autorizadas (emisores) [SIII§2]; SGC y organismos descentralizados de la UE: personas autorizadas (emisores) [SIII§2]; Directores Generales, Secretario General/Alto Representante y Secretario General Adjunto. Los emisores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años como mínimo, para comprobar si la clasificación original sigue siendo pertinente [SIII§10].	La clasificación SECRET UE se aplicará a los documentos SECRET UE y, cuando proceda, se pondrá la indicación ESDP (PESD), por medios mecánicos y a mano [SII§8]. Las clasificaciones de la UE aparecerán en la parte central, superior e inferior, de cada página; todas las páginas irán numeradas. Todos los documentos 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 [SVII§1].	La desclasificación o recalificación depende únicamente del emisor o del Secretario General/Alto Representante, que informarán de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [SIII§9]. Los documentos SECRET UE serán destruidos por el registro encargado de su custodia, bajo la supervisión de una persona con habilitación de seguridad. Los documentos SECRET UE destruidos serán enumerados en certificados de destrucción que guardará el registro, junto con los impresos de distribución, durante al menos tres años [SVII§32].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [SVII§31]. Los documentos SECRET UE, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos SECRET UE, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos; la destrucción se hará quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [SVII§§31,32].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
CONFIDENTIEL UE (UE confidencial): 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 [SII§3].	Si existe la probabilidad de que la puesta en peligro de materiales marcados CONFIDENTIEL UE: — 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 a 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 investigación de delitos graves o facilite su comisión; — 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.	Estados miembros: personas autorizadas (emisores) [SIII§2]; SGC y organismos descentralizados de la UE: personas autorizadas (emisores) [SIII§2]; Directores Generales, Secretario General/Alto Representante y Secretario General Adjunto. Los emisores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años como mínimo, para comprobar si la clasificación original sigue siendo pertinente [SIII§10].	La clasificación CONFIDENTIEL UE se aplicará a los documentos CONFIDENTIEL UE y, cuando proceda, se pondrá la indicación ESDP (PESD), por medios mecánicos y a mano [SII§8]. Las clasificaciones de la UE figurarán en la parte central, superior e inferior, de cada página; todas las páginas irán numeradas. Todos los documentos llevarán número de referencia y fecha. Todos los anexos y documentos adjuntos se indicarán en la primera página [SVII§1].	La desclasificación o recalificación depende únicamente del emisor o del Secretario General/Alto Representante, que informarán de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [SIII§9]. Los documentos CONFIDENTIEL UE serán destruidos por el registro encargado de su custodia, bajo la supervisión de una persona habilitada. Su destrucción se registrará de acuerdo con las normas nacionales y, en el caso de la SGC o de los organismos descentralizados de la UE, según las instrucciones del Secretario General/Alto Representante o del Secretario General Adjunto [SVII§33].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [SVII§31]. Los documentos CONFIDENTIEL UE, incluido todo el material sobrante clasificado que se haya utilizado para preparar documentos CONFIDENTIEL UE, como copias defectuosas, borradores de trabajo, notas mecanografiadas y papel carbón, serán destruidos; la destrucción se hará quemándolos, convirtiéndolos en pasta, triturándolos o reduciéndolos de cualquier otro modo a un estado en que sean irreconocibles e irreconstruibles [SVII§§31, 33].

Clasificación	Cuándo	Quién	Marcados	Recalificación/Desclasificación/Destrucción	
				Quién	Cuándo
RESTREINT UE (UE reservado): 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 [SII§4].	Si existe la probabilidad de que la puesta en peligro de materiales marcados RESTREINT UE: — afecte desfavorablemente a las relaciones diplomáticas; — causar considerable sufrimiento a individuos; — 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 facilite ganancias o ventajas indebidas a individuos o empresas; — quebrante el debido esfuerzo por mantener la reserva de la información facilitada por terceros; — dificulte la investigación o facilite la comisión de delitos; — ponga en desventaja a la UE o a sus Estados miembros en negociaciones comerciales o en actuaciones de otra índole con terceros; — ponga obstáculos al desarrollo o al funcionamiento efectivos de políticas prioritarias de la UE; — menoscabe la adecuada gestión de la UE y sus operaciones.	Estados miembros: personas autorizadas (emisores) [SIII§2]; SGC y organismos descentralizados de la UE: personas autorizadas (emisores) [SIII§2], Directores Generales, Secretario General/Alto Representante y Secretario General Adjunto. Los emisores deberán especificar una fecha o plazo en que el contenido pueda ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años como mínimo, para comprobar si la clasificación original sigue siendo necesaria [SIII§10].	La clasificación RESTREINT UE se aplicará a los documentos RESTREINT UE y, cuando proceda, se pondrá la indicación ESDP (PESD), por medios mecánicos y a mano [SII§8]. Las clasificaciones de la UE figurarán en la parte central, superior e inferior, de cada página; todas las páginas irán numeradas. Todos los documentos llevarán número de referencia y fecha [SVII§1].	La desclasificación o recalificación depende únicamente del autor o del Secretario General/Alto Representante, que informarán de la modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo [SIII§9]. Los documentos RESTREINT UE serán destruidos por el registro encargado de su custodia, de acuerdo con las normas nacionales y, en el caso de la SGC y de los organismos descentralizados de la UE, según las instrucciones del Secretario General/Alto Representante o del Secretario General Adjunto [SVII§34].	Las copias y documentos sobrantes que ya no sean necesarios serán destruidos [SVII§31].

Apéndice 4

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 Consejo la autoridad para entregar información clasificada de la UE a países que no sean signatarios del Tratado de la Unión Europea y a organizaciones internacionales cuyas política y normativa de seguridad son muy similares a las de la UE.

2. El Consejo podrá delegar la decisión de entregar información clasificada. Al hacerlo, el Consejo declarará la naturaleza de la información que puede entregarse y su nivel de clasificación, que, normalmente, no será superior a CONFIDENTIEL UE.

3. Sin perjuicio de que se celebre un acuerdo de seguridad, las solicitudes de entrega de información clasificada de la UE serán presentadas al Secretario General/Alto Representante por los órganos de seguridad de los países u organizaciones internacionales interesados, que expondrán la finalidad con que solicitan la entrega de la información y la naturaleza de la información clasificada cuya entrega se solicita.

   También podrán presentar solicitudes al efecto los Estados miembros o los organismos descentralizados de la UE que consideren conveniente la entrega de determinada información clasificada de la UE; expondrán el uso que van a dar a la información y las ventajas que supone su entrega para la UE, indicando la naturaleza y nivel de clasificación de la información cuya entrega solicitan.

4. La SGC estudiará la solicitud y:

   — recabará la opinión del Estado miembro o, en su caso, del organismo descentralizado de la UE emisor de la información 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 a las ANS respecto de la confianza que puede depositarse en los países u organizaciones internacionales beneficiarios.

5. La SGC remitirá al Consejo la solicitud, junto con la recomendación de la Oficina de Seguridad, para que decida.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

6. El Secretario General/Alto Representante notificará a los países u organizaciones internacionales beneficiarios la decisión del Consejo de autorizar la entrega de información clasificada de la UE, y les remitirá tantos ejemplares de las presentes normas de seguridad como considere necesarios. Si la solicitud fue cursada por un Estado miembro, éste notificará al beneficiario que la entrega se ha autorizado.

   La decisión de entregar no entrará en vigor hasta que los beneficiarios no 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 CONFIDENTIEL UE 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 con arreglo a lo dispuesto en la sección VII de las presentes normas de seguridad. 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 el Consejo incluye material clasificado TRÈS SECRET UE/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 las disposiciones de la sección VIII de las presentes normas de seguridad.

9. *Inscripción en el registro*

No bien se reciba en un registro un documento clasificado CONFIDENTIEL UE 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 emisor 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 VI de las presentes normas de seguridad. Se enviarán copias de los certificados de destrucción de los documentos SECRET UE y TRÈS SECRET UE/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 los documentos*

Se tomarán 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 CONFIDENTIEL UE o SECRET UE, 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 TRÈS SECRET UE/EU TOP SECRET sólo podrá ser autorizada por la autoridad emisora, que especificará el número de copias autorizadas. Si no puede determinarse dicha autoridad emisora, la petición se remitirá a la Oficina de Seguridad de la SGC.

13. *Quebrantamientos de la seguridad*

Cuando se haya producido o se sospeche que se ha producido un quebrantamiento 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 del quebrantamiento de la seguridad;

b) notificar el hecho a la Oficina de Seguridad de la SGC, a la ANS y a la autoridad emisora, o, si todavía no se ha informado a esta última, hacerlo constar claramente;

c) tomar medidas para reducir al mínimo los efectos del quebrantamiento 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 SGC para impedir que el hecho vuelva a suceder.

14. *Inspecciones*

Se permitirá a la Oficina de Seguridad de la SGC, 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 5

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 Consejo 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. En principio, se limita a la información clasificada hasta el nivel SECRET UE inclusive, y no incluye la información nacional específicamente reservada a los Estados miembros ni las categorías de la información clasificada de la UE protegidas por marcados especiales.

2. El Consejo podrá delegar su decisión. Al hacerlo, dentro de los límites definidos en el apartado 1, declarará la naturaleza de la información que puede entregarse y su nivel de clasificación, que no será superior a RESTREINT UE.

3. Sin perjuicio de que se celebre un acuerdo de seguridad, las solicitudes de entrega de información clasificada de la UE serán presentadas al Secretario General/Alto Representante por los órganos de seguridad de los países u organizaciones internacionales interesados, que expondrán la finalidad con que solicitan la entrega de la información y la naturaleza de la información clasificada cuya entrega se solicita.

   También podrán presentar solicitudes al efecto los Estados miembros o los organismos descentralizados de la UE que consideren conveniente la entrega de determinada información clasificada de la UE; expondrán el uso que van a dar a la información y las ventajas que supone su entrega para la UE, indicando la naturaleza y categoría de la información cuya entrega solicitan.

4. La SGC estudiará la solicitud y:

   — recabará la opinión del Estado miembro o, en su caso, del organismo descentralizado de la UE emisor de la información cuya entrega se solicita;

   — entablará contactos preliminares con los organismos de seguridad de los países u organizaciones internacionales beneficiarios, 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 Comité de Seguridad del Consejo 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 técnico del Comité de Seguridad.

5. El dictamen técnico del Comité de Seguridad del Consejo 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.);

   — la recalificación o desclasificación, por la autoridad emisora, antes de que la información se entregue a los países u organizaciones internacionales beneficiarios [1].

[1] Esto supone la aplicación, por la autoridad emisora, del procedimiento mencionado en el apartado 9 de la sección III a todas las copias que circulen dentro de la UE.

6. El Secretario General/Alto Representante remitirá al Consejo, para que éste decida, la solicitud y el dictamen técnico del Comité de Seguridad del Consejo obtenido por la Oficina de Seguridad de la SGC.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

7. El Secretario General/Alto Representante notificará a los países u organizaciones internacionales beneficiarios la decisión del Consejo de autorizar la entrega de información clasificada de la UE, junto con un cuadro comparativo de las clasificaciones vigentes en la UE y en los países u organizaciones de que se trate. Si la solicitud fue cursada por un Estado miembro, éste notificará al beneficiario que la entrega se ha autorizado.

   La decisión de entregar no entrará en vigor hasta que los beneficiarios no 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 el Consejo.

8. Se establecerán las siguientes normas de protección, salvo en el caso de que el Consejo, después de recibir el dictamen técnico del Comité de Seguridad del Consejo, decida un procedimiento especial para tratar los documentos clasificados de la UE (supresión de la mención de la clasificación de la UE, de los marcados específicos, etc.).

   En este caso, se procederá a adaptar las normas.

9. *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 UE 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 a título informativo al Secretario General/Alto Representante.

10. *Transmisión de documentos*

   a) Los procedimientos prácticos para la transmisión de documentos se decidirán por acuerdo entre la Oficina de Seguridad de la SGC y los organismos de seguridad de los países u organizaciones internacionales destinatarios con arreglo a las disposiciones que figuran en la sección VII de las presentes normas. Indicarán, en particular, las direcciones concretas a las que deben remitirse los documentos, así como los servicios de mensajería o correo utilizados para la transmisión de la información clasificada de la UE.

   b) Los documentos clasificados CONFIDENTIEL UE y de nivel superior se transmitirán bajo doble pliego. El sobre interior llevará la marca «UE», junto con la clasificación de seguridad. Con cada documento clasificado se incluirá un impreso de recibo que no se clasificará 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.

11. *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 UE, 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.

12. *Devolución de documentos*

Cuando el destinatario devuelva un documento clasificado al Consejo o al Estado miembro que lo ha entregado, procederá de la forma que se indica en el apartado 10.

13. *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 CONFIDENTIEL UE o de nivel superior, ni hacerse extractos sin la autorización de la Oficina de Seguridad de la SGC.

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

14. *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 órgano 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.

15. *Quebrantamientos de la seguridad*

Cuando se haya producido o se sospeche que se ha producido un quebrantamiento 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 SGC o a la ANS del Estado miembro que tomó la iniciativa de transmitir los documentos (con copia a la Oficina de Seguridad de la SGC);

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.

16. *Inspecciones*

Se permitirá a la Oficina de Seguridad de la SGC, 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.

17. *Informe*

Mientras el país u organización 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 6

Directrices para la entrega de información clasificada de la UE a terceros países u organizaciones internacionales

Cooperación de nivel 3

PROCEDIMIENTO

1. Ocasionalmente, el Consejo podrá querer cooperar, en determinadas circunstancias especiales, con países u organizaciones que no puedan ofrecer las garantías exigidas por las presentes normas de seguridad, pero que podrán solicitar cooperación para la entrega de información clasificada de la UE. Dicha entrega afectará exclusivamente a información nacional específicamente reservada a los Estados miembros.

2. En estas circunstancias especiales, las solicitudes de cooperación con la UE, tanto de terceros países u organizaciones internacionales como propuestas por los Estados miembros o, cuando proceda, por organismos descentralizados de la UE, será estudiada en primer lugar, en lo que se refiere al fondo, por el Consejo; éste, si fuera necesario, recabaría la opinión de los Estados miembros o de los organismos descentralizados emisores de la información. El Consejo 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.

3. Si el Consejo se muestra favorable, incumbirá al Secretario General/Alto Representante convocar al Comité de Seguridad del Consejo o recabar información de las ANS de los Estados miembros, si ha lugar mediante el procedimiento de aprobación tácita, con el fin de obtener el dictamen técnico del Comité de Seguridad.

4. El dictamen técnico del Comité de Seguridad del Consejo incluirá 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, cuando proceda, habida cuenta de su naturaleza;

   c) la recalificación o desclasificación de la información por la autoridad emisora antes de entregarla a los países u organizaciones internacionales interesados ([1]);

   d) procedimientos para tratar los documentos que hayan de entregarse (véase el apartado 5);

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

5. 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 Comité de Seguridad del Consejo 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 (véanse ejemplos en el apartado 14).

6. La Oficina de Seguridad de la SGC remitirá al Consejo el dictamen técnico del Comité de Seguridad y adjuntará, si fuera necesario, las delegaciones de autoridad propuestas que sean necesarias para el cumplimiento de la misión, especialmente en circunstancias de urgencia.

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

([1]) Esto supone la aplicación, por la autoridad emisora, del procedimiento mencionado en el apartado 4 de la Sección III a todas las copias que circulen en la UE.

8. A modo de referencia, la Oficina de Seguridad de la SGC distribuirá a todos los Estados miembros y, si procede, a los organismos descentralizados de la UE interesados, un cuadro en que se resuma la naturaleza y clasificación de la información y figure la relación de las organizaciones y países a los que dicha información puede entregarse, con arreglo a la decisión del Consejo.

9. La ANS del Estado miembro que haya efectuado la entrega, o bien la Oficina de Seguridad de la SGC, tomará todas las medidas necesarias para facilitar la evaluación de cualquier daño consiguiente y la revisión de los procedimientos.

10. Siempre que se modifiquen las condiciones de la cooperación, deberá informarse al Consejo.

NORMAS DE SEGURIDAD QUE DEBERÁN APLICAR LOS BENEFICIARIOS

11. El Secretario General/Alto Representante notificará a los Estados u organizaciones internacionales beneficiarios la decisión del Consejo de autorizar la entrega de información clasificada de la UE, junto con las normas detalladas de protección propuestas por el Comité de Seguridad del Consejo y aprobadas por el Consejo. Si la solicitud se hizo a través de un Estado miembro, éste notificará al beneficiario que la entrega se ha autorizado.

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

— no utilizarán la información para fines distintos de la cooperación decidida por el Consejo;

— darán a la información la protección exigida por el Consejo.

12. *Transmisión de documentos*

a) Los procedimientos prácticos para la transmisión de documentos se decidirán por acuerdo entre la Oficina de Seguridad de la SGC 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 CONFIDENTIEL UE 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.

13. *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 UE, 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.

14. *Uso y protección de la información clasificada objeto de intercambio*

a) La información clasificada SECRET UE 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 SECRET UE se remitirá mediante valija diplomática, servicios de correo de seguridad y telecomunicaciones de seguridad. Sólo podrán hacerse copias de los documentos SECRET UE con el acuerdo escrito de la autoridad emisora. Todas las copias serán registradas y controladas. Se entregarán recibos de todas las operaciones relativas a los documentos clasificados SECRET UE.

b) La información clasificada CONFIDENTIEL UE 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 CONFIDENTIEL UE 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 RESTREINT UE 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.

15. *Destrucción*

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

16. *Quebrantamientos de la seguridad*

Si la información clasificada CONFIDENTIEL UE o SECRET UE 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. Si la investigación arroja resultados positivos, deberá informarse a la autoridad emisora. Deberán adoptarse las medidas necesarias para subsanar procedimientos o métodos de almacenamiento inadecuados, si han dado origen a un riesgo. El Secretario General/Alto Representante del Consejo o la ANS del Estado miembro que haya entregado la información podrá pedir al beneficiario información sobre la investigación.