IV

(Información)

INFORMACIÓN PROCEDENTE DE LAS INSTITUCIONES, ÓRGANOS Y ORGANISMOS DE LA UNIÓN EUROPEA

PARLAMENTO EUROPEO

DECISIÓN DE LA MESA DEL PARLAMENTO EUROPEO

de 6 de junio de 2011

sobre la reglamentación sobre el tratamiento de la información confidencial por el Parlamento Europeo

(2011/C 190/02)

LA MESA DEL PARLAMENTO EUROPEO,

Visto el artículo 23, apartado 12, del Reglamento del Parlamento Europeo,

Considerando lo siguiente:

(1) A la luz del nuevo Acuerdo marco sobre las relaciones entre el Parlamento Europeo y la Comisión Europea [1], firmado el 20 de octubre de 2010 («el Acuerdo Marco») es necesaria la revisión de la Decisión de la Mesa, de 13 de noviembre de 2006, relativa a la reglamentación sobre la tramitación administrativa de los documentos confidenciales.

(2) El Tratado de Lisboa atribuye nuevas tareas al Parlamento Europeo y, a fin de desarrollar las actividades del Parlamento en aquellos ámbitos que requieren cierto grado de confidencialidad, es necesario establecer principios básicos, normas mínimas de seguridad y procedimientos adecuados para el tratamiento por el Parlamento Europeo de la información confidencial, incluida la información clasificada.

(3) La reglamentación establecida en la presente Decisión tiene por objeto garantizar unas normas equivalentes de protección y la compatibilidad con las normas adoptadas por otras instituciones, órganos y organismos establecidos en virtud o sobre la base de los Tratados o por los Estados miembros, a fin de facilitar el correcto funcionamiento del proceso de toma de decisiones de la Unión Europea.

(4) Las disposiciones de la presente Decisión se entienden sin perjuicio del artículo 15 del Tratado de Funcionamiento de la Unión Europea (TFUE) y el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión [2].

(5) Las disposiciones de la presente Decisión se entienden sin prejuicio del artículo 16 del TFUE y el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [3].

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Objetivo

La presente Decisión regula la creación, la recepción, la transmisión y el almacenamiento de información confidencial por el Parlamento Europeo, con miras a la protección adecuada de su naturaleza confidencial. Por medio de la presente Decisión se aplica, en particular, el anexo 2 del Acuerdo Marco.

[1] DO L 304 de 20.11.2010, p. 47.

[2] DO L 145 de 31.5.2001, p. 43.

[3] DO L 8 de 12.1.2001, p. 1.

Artículo 2

Definiciones

A los efectos de la presente Decisión:

a) por «información» se entenderá toda información escrita u oral, cualquiera que sea el soporte o el autor;

b) por «información confidencial» se entenderá la «información clasificada de la UE», y «otra información confidencial» no clasificada;

c) por «información clasificada de la UE» se entenderá toda información y material, clasificados como «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET», «CONFIDENTIEL UE/EU CONFIDENTIAL» o «RESTREINT UE/EU RESTRICTED», cuya divulgación no autorizada pueda causar perjuicio en distintos grados a los intereses de la UE, o a los de uno o más de los Estados miembros, ya se origine dicha información en las instituciones, órganos y organismos establecidos en virtud o sobre la base de los Tratados o proceda de los Estados miembros, terceros países u organizaciones internacionales. A este respecto:

— «TRÈS SECRET UE/EU TOP SECRET» es la clasificación correspondiente a la información y el material cuya divulgación no autorizada puede causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión o de uno o más de los Estados miembros,

— «SECRET UE/EU SECRET» es la clasificación correspondiente a la información y el material cuya divulgación no autorizada puede suponer un perjuicio grave para los intereses esenciales de la Unión o de uno o más de los Estados miembros,

— «CONFIDENTIEL UE/EU CONFIDENTIAL» es la clasificación correspondiente a la información y el material cuya divulgación no autorizada puede suponer un perjuicio para los intereses esenciales de la Unión o de uno o más de los Estados miembros,

— «RESTREINT UE/EU RESTRICTED» es la clasificación correspondiente a la información y el material cuya divulgación no autorizada puede resultar desventajosa para los intereses de la Unión o de uno o más de los Estados miembros;

d) por «otra información confidencial» se entenderá cualquier otra información confidencial no clasificada, incluida la información cubierta por normas de protección de datos o por la obligación de secreto profesional, originada en el Parlamento Europeo o enviada por otras instituciones, órganos y organismos establecidos en virtud o sobre la base de los Tratados o por Estados miembros al Parlamento Europeo;

e) por «documento» se entenderá toda información registrada, independientemente de su soporte físico o características;

f) por «material» se entenderá todo documento, máquina o aparato, producido o en proceso de producción;

g) por «necesidad de conocer» se entenderá la necesidad de una persona de tener acceso a información confidencial para poder desempeñar una función o tarea oficial;

h) por «autorización» se entenderá la decisión (decisión de habilitación) del Presidente, si se trata de diputados al Parlamento Europeo, y del Secretario General, si se trata de funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos, de permitir a una persona el acceso a información clasificada de la UE hasta un nivel determinado, sobre la base del resultado positivo de una comprobación de seguridad (investigación), llevada a cabo por una autoridad nacional de acuerdo con la legislación nacional y con arreglo a lo dispuesto en el anexo I, parte 2;

i) por «recalificación» se entenderá la disminución del nivel de clasificación;

j) por «desclasificación» se entenderá la supresión de toda clasificación;

k) por «autor» se entenderá la persona debidamente autorizada que ha redactado información clasificada de la UE o cualquier otra información confidencial;

l) por «indicaciones de seguridad» se entenderá las medidas técnicas de aplicación establecidas en el anexo II [1].

Artículo 3

Principios básicos y normas mínimas

1. El tratamiento de la información confidencial por el Parlamento Europeo se regirá por los principios básicos y las normas mínimas establecidos en el anexo I, parte 1.

2. El Parlamento Europeo establecerá un Sistema de Gestión de la Seguridad de la Información (SGSI) con arreglo a dichos principios básicos y normas mínimas cuyo objetivo será facilitar la labor parlamentaria y administrativa y garantizar al mismo tiempo la protección de toda información confidencial tratada por el Parlamento Europeo, respetando plenamente las pautas establecidas por el autor de la información, establecidas en las indicaciones de seguridad.

El tratamiento de información confidencial por medio de sistemas de información automáticos del Parlamento Europeo se aplicará de acuerdo con el concepto de aseguramiento de la información y se establecerá en las indicaciones de seguridad.

[1] El anexo debe aprobarse.

3. Los diputados al Parlamento Europeo podrán consultar la información clasificada, hasta el nivel «CONFIDENTIEL UE/EU CONFIDENTIAL» incluido, sin necesidad de habilitación de seguridad. Para consultar información clasificada como «CONFIDENTIEL UE/EU CONFIDENTIAL», deberán firmar una declaración solemne de que no divulgarán el contenido de dicha información a terceros. La información con una clasificación superior al nivel «CONFIDENTIEL UE/EU CONFIDENTIAL» sólo se pondrá a disposición de los diputados con el nivel adecuado de habilitación de seguridad.

4. Los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos podrán consultar la información confidencial si tienen una necesidad de conocer reconocida y la información clasificada de un nivel superior a «RESTREINT UE/EU RESTRICTED» si disponen del nivel adecuado de habilitación de seguridad.

Artículo 4

Emisión de información confidencial y tratamiento administrativo por el Parlamento Europeo

1. El Presidente del Parlamento Europeo, los presidentes de las comisiones parlamentarias interesadas y el Secretario General o cualquier persona debidamente autorizada por éste por escrito podrán emitir información confidencial o clasificar información, según lo establecido en las indicaciones de seguridad.

2. Al emitir información clasificada, el autor aplicará los niveles adecuados de clasificación con arreglo a las normas y definiciones internacionales previstas en el anexo I. El autor determinará también, por norma general, qué destinatarios están autorizados para consultar la información con arreglo al nivel de clasificación. Esta información se comunicará al Servicio de Información Confidencial (SIC) al depositar el documento en dicho servicio.

3. La información confidencial cubierta por la obligación de secreto profesional deberá tratarse con arreglo a las instrucciones de tratamiento definidas en las indicaciones de seguridad.

Artículo 5

Recepción de información confidencial por el Parlamento Europeo

1. La información confidencial recibida por el Parlamento Europeo se transmitirá de la manera siguiente:

— la información clasificada de la UE clasificada como «RESTREINT UE/EU RESTRICTED» y otra información confidencial, a la secretaría de la instancia parlamentaria o el cargo público que haya presentado la solicitud,

— la información clasificada de la UE clasificada como «CONFIDENTIEL UE/ EU CONFIDENTIAL EU» o superior, al SIC.

2. El registro, el almacenamiento y la trazabilidad de la información confidencial serán asumidos bien por la secretaría de la instancia parlamentaria o el cargo público que haya recibido la información bien por el SIC.

3. Al tratarse de información confidencial transmitida por la Comisión sobre la base del Acuerdo Marco, las modalidades acordadas en el sentido de su anexo 2, punto 3.2 (establecidas de común acuerdo y referentes a los destinatarios, procedimientos de consulta —es decir, sala de lectura segura— y, reuniones a puerta cerrada u otros asuntos.), para preservar la confidencialidad de la información deberán depositarse junto con la información confidencial en la secretaría de la instancia parlamentaria o el cargo público, o en el SIC, cuando la información tenga una clasificación «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior.

4. Las disposiciones a las que se hace referencia en al apartado 3 podrán aplicarse también, mutatis mutandis, para la transmisión de información confidencial por otras instituciones, órganos y organismos de la establecidos en virtud o sobre la base de los Tratados o por los Estados miembros.

5. La transmisión al Parlamento Europeo de información clasificada de la UE con el nivel «TRÈS SECRET UE/EU TOP SECRET» estará sometida a otras disposiciones, que se acordarán entre la instancia parlamentaria o el cargo público que haya presentado la solicitud de información y la institución o el Estado miembro que la transmitan. La Conferencia de Presidentes deberá constituir un comité de supervisión. Su objetivo será garantizar un nivel de protección adecuado a ese nivel de clasificación.

Artículo 6

Transmisión de información clasificada de la UE a terceros por el Parlamento Europeo

El Parlamento Europeo podrá transmitir, con sujeción al consentimiento del autor, información clasificada de la UE a otras instituciones, órganos y organismos establecidos virtud o sobre la base de los Tratados o a Estados miembros, siempre y cuando garanticen que, cuando se trate este tipo de información, se cumplan en sus servicios y locales normas equivalentes a las normas establecidas en la presente Decisión.

Artículo 7

Almacenamiento y consulta de información confidencial en zonas protegidas (salas de lectura seguras)

1. Las salas de lectura seguras permitirán un almacenamiento seguro y no contendrán máquinas fotocopiadoras, teléfonos, fax, escáneres ni otro medio técnico de reproducción o transmisión de documentos.

2. Las condiciones siguientes regirán el acceso a la sala de lectura segura:

a) Sólo tendrán acceso las personas siguientes:

— los diputados al parlamento Europeo, los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos debidamente identificados, con arreglo a las disposiciones a que se refieren el artículo 4, apartado 2, y el artículo 5, apartados 3 y 4,

— los funcionarios del Parlamento Europeo gestores del SIC,

— en caso necesario, los funcionarios del Parlamento Europeo competentes en materia de seguridad y prevención de incendios.

La limpieza de la zona de seguridad sólo se llevará a cabo en presencia y bajo estrecha vigilancia de un funcionario del SIC.

b) Toda persona que desee acceder a la información confidencial comunicará su nombre con antelación al SIC. El SIC comprobará la identidad de cada persona que presente una solicitud de consulta de información confidencial y verificará, en su caso, si dicha persona cuenta con el nivel necesario de habilitación de seguridad y está autorizada para consultarla con arreglo a las disposiciones a que se refieren el artículo 4, apartado 2, y el artículo 5, apartados 3 y 4.

c) el SIC estará habilitado para denegar el acceso a la sala a toda persona no autorizada para ingresar ella, con arreglo a las letras a) y b). Toda objeción a la decisión del SIC se someterá al Presidente, en el caso de los diputados al Parlamento Europeo, y al Secretario General, en los demás casos.

3. Las condiciones siguientes regirán la consulta de información confidencial en la sala de lectura segura:

a) las personas autorizadas para consultar la información que hayan presentado la solicitud a que se refiere el apartado 2, letra b), deberán personarse en el SIC.

Salvo en casos excepcionales, (por ejemplo, numerosas solicitudes de consulta en un breve período de tiempo), la consulta de información confidencial en la sala de lectura segura sólo se autorizará a una única persona al mismo tiempo, en presencia de un funcionario del SIC.

Dicho funcionario informará de sus obligaciones a la persona autorizada para consultar la información confidencial y, en particular, le pedirá que firme una declaración jurada en la que se comprometa a no revelar su contenido a terceros.

b) durante el proceso de consulta estará prohibido el contacto con el exterior (incluido el uso del teléfono u otros medios técnicos), la toma de notas y el fotocopiado o fotografiado de la información confidencial consultada.

c) antes de autorizar a una persona a abandonar la sala de lectura segura, el funcionario del SIC mencionado en la letra a) se asegurará de que la información confidencial consultada está todavía en la sala, intacta y completa.

4. En caso de incumplimiento de las normas arriba expuestas, el funcionario responsable del SIC informará al Secretario General, que informará a su vez al Presidente en caso de que el autor del incumplimiento sea un diputado al Parlamento Europeo.

Artículo 8

Normas mínimas para otras consultas de información confidencial

1. Por lo que respecta al tratamiento administrativo de información confidencial en una reunión a puerta cerrada, la secretaría de la instancia parlamentaria o el cargo público responsable de la reunión garantizará lo siguiente:

— que sólo se permita la entrada en la sala a las personas que estén designadas para participar en la reunión y cuenten con el nivel necesario de habilitación de seguridad,

— que todos los documentos estén numerados, se distribuyan al comienzo de la reunión y se recojan al final, y que no se tomen notas ni se hagan fotocopias ni fotografías de dichos documentos,

— que en el acta de la reunión no se haga mención alguna del contenido de la discusión de la información tratada según el procedimiento confidencial,

— que la información confidencial facilitada verbalmente a los destinatarios en el Parlamento Europeo se someta a un nivel de protección equivalente al de la información confidencial facilitada por escrito; podrá incluirse una declaración solemne de los destinatarios de dicha información de no divulgar su contenido a terceros.

2. Se aplicarán las reglas siguientes al tratamiento administrativo de información confidencial por la secretaría de la instancia parlamentaria o el cargo público fuera de la reunión a puerta cerrada:

— los documentos en papel se transmitirán en persona al responsable de la secretaría, que los registrará y facilitará un acuse de recibo,

— tales documentos se conservarán en un lugar cerrado, bajo la responsabilidad de la secretaría, cuando no estén siendo utilizados,

— sin perjuicio del tratamiento administrativo de la información confidencial en una reunión a puerta cerrada como se establece en el apartado 1, en ningún caso se duplicará, se guardará en otro soporte o se transmitirá a persona alguna,

— el acceso a tales documentos se restringirá a los destinatarios de los mismos y, de conformidad con las disposiciones a que se refieren el artículo 4, apartado 2, el artículo 5, apartado 3, y el artículo 5, apartado 4, estará sometido a la supervisión de la secretaría,

— la secretaría llevará un registro de las personas que hayan consultado los documentos, junto con la fecha y la hora de tales consultas. Dicho registro se transmitirá al SIC para la elaboración del informe anual mencionado en el artículo 12.

Artículo 9

Archivo de información confidencial

1. El Parlamento Europeo dispondrá en sus locales de un sistema de archivo seguro.

La información confidencial depositada con carácter definitivo en el SIC o en la secretaría de la instancia parlamentaria o el cargo público se trasladará al archivo seguro del SIC seis meses después de su última consulta y, a más tardar, un año después de haber sido depositada.

2. El SIC se encargará de la gestión de los archivos seguros, de conformidad con los criterios de archivo habituales.

3. La información confidencial contenida en los archivos seguros podrá consultarse en las siguientes condiciones:

— sólo estarán autorizadas para consultar esta información las personas identificadas, nominalmente o con arreglo a su cargo, en la ficha de acompañamiento cumplimentada al depositar la información,

— la solicitud de consulta de información confidencial deberá dirigirse al SIC, que se encargará de trasladar el documento en cuestión a la sala de lectura segura,

— se aplicarán los procedimientos y condiciones relativos a la consulta de información confidencial previstos en el artículo 7.

Artículo 10

Recalificación y desclasificación de la información clasificada de la UE

1. La información clasificada de la UE podrá recalificarse o desclasificarse únicamente con la autorización del autor y, en caso necesario, tras consultar a las demás partes interesadas. La recalificación o desclasificación se confirmará por escrito. El autor se encargará de informar de la modificación a sus destinatarios; estos, por su parte, se encargarán de informar de dicha modificación a los destinatarios subsiguientes a quienes se haya enviado el documento o una copia del mismo. Siempre que sea posible, los autores deberán especificar en los documentos clasificados la fecha, el plazo o el suceso a partir de los cuales el contenido podrá ser recalificado o desclasificado. En caso contrario, revisarán los documentos cada cinco años, a más tardar, para comprobar si la clasificación original sigue siendo necesaria.

2. La desclasificación de los documentos de los archivos seguros tendrá lugar, a más tardar, después de 30 años, de conformidad con lo dispuesto en el Reglamento (CEE, Euratom) nº 354/83 del Consejo, de 1 de febrero de 1983, relativo a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía Atómica ([1]). La desclasificación la llevará a cabo el autor de la información clasificada o el servicio que en ese momento sea responsable, de conformidad con el anexo 1, parte 1, sección 10.

Artículo 11

Quebrantamientos relativos a la información confidencial

1. Los quebrantamientos de la confidencialidad en general, y de la presente Decisión en particular, implicarán, en el caso de los diputados al Parlamento Europeo, la aplicación de las disposiciones sancionadoras pertinentes previstas en el Reglamento del Parlamento Europeo.

2. Los quebrantamientos por parte del personal darán lugar a la aplicación de los procedimientos y sanciones previstos respectivamente en el Estatuto de los funcionarios y en el régimen aplicable a otros agentes de la Unión Europea, establecidos en el Reglamento (CEE, Euratom, CECA) nº 259/68 ([2]) («el Estatuto de los funcionarios»).

3. El Presidente y el Secretario General organizarán todas las investigaciones necesarias.

Artículo 12

Adaptación de la presente decisión y de las normas de aplicación e informe anual sobre la aplicación de la presente Decisión

1. El Secretario General propondrá toda adaptación necesaria de la presente Decisión y de los anexos por los que se aplica, y someterá tales propuestas a la decisión de la Mesa.

2. El Secretario General presentará a la Mesa un informe anual sobre la aplicación de la presente Decisión.

([1]) DO L 43 de 15.2.1983, p. 1.
([2]) DO L 56 de 4.3.1968, p. 1.

Artículo 13

Disposiciones transitorias y finales

1. La información confidencial existente en el SIC o en los archivos con anterioridad a la aplicación de la presente Decisión se clasificarán por defecto como «RESTREINT UE/EU RESTRICTED», a no ser que su autor decida no clasificarla o clasificarla a un nivel más alto o con un marcado en el plazo de un año a partir de la fecha de entrada en vigor de la presente Decisión.

2. Si su autor decide asignar a la información confidencial una clasificación más alta, la información se clasificará al nivel más bajo posible por el autor o sus delegados, en colaboración con el SIC y de conformidad con los criterios establecidos en el anexo I.

3. Queda derogada la Decisión de la Mesa de 13 de noviembre de 2006 sobre la reglamentación sobre la tramitación administrativa de los documentos confidenciales.

4. Queda derogada la decisión de la Mesa, de 24 de octubre de 2005, por la que se confiere mandato al Secretario General para constituir un comité de desclasificación y tomar decisiones relativas a la desclasificación.

Artículo 14

Entrada en vigor

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

2. Será aplicable a partir del 1 de julio de 2011.

ANEXO I

PARTE 1

PRINCIPIOS BÁSICOS Y NORMAS MÍNIMAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL

1. Introducción

Las presentes disposiciones establecen los principios básicos y las normas mínimas de seguridad que deberán cumplir el Parlamento Europeo, en todos sus lugares de trabajo, y todos los destinatarios de información clasificada de la UE y otra información confidencial, a fin de salvaguardar la seguridad y garantizar a todas las personas implicadas el establecimiento de una norma común de protección. Dichas disposiciones están complementadas por la reglamentación sobre el tratamiento de la información confidencial por las comisiones parlamentarias y otras instancias parlamentarias o cargos públicos.

2. Principios generales

La política de seguridad del Parlamento Europeo forma parte integrante de su política general de gestión interna y está basada, por lo tanto, en los principios que rigen su política general. Dichos principios incluyen la legalidad, transparencia, responsabilidad y subsidiariedad y proporcionalidad.

El principio de legalidad conlleva la necesidad de permanecer estrictamente en el marco jurídico a la hora de ejecutar las funciones de seguridad y de ajustarse a los requisitos jurídicos aplicables. Significa también que las responsabilidades en materia de seguridad deben basarse en disposiciones legales adecuadas. Son plenamente aplicables las disposiciones del Estatuto de los funcionarios y, especialmente, su artículo 17, relativo a la obligación del personal de abstenerse de divulgar sin autorización información que haya recibido en relación con sus funciones, y su título VI, sobre el régimen disciplinario. También significa, por último, que las infracciones a la seguridad que son responsabilidad del Parlamento Europeo deben tratarse de forma coherente con la política del Parlamento Europeo en materia de medidas disciplinarias.

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

El principio de responsabilidad significa que se definirán claramente las responsabilidades en el ámbito de la seguridad. Conlleva además la necesidad de de un seguimiento regular, a fin de comprobar si se asumen correctamente dichas responsabilidades.

El principio de subsidiariedad significa que la seguridad se organizará al nivel más bajo posible y más próximo posible de las Direcciones Generales y los servicios del Parlamento Europeo. El principio de proporcionalidad implica que las actividades relacionadas con la seguridad se limitarán exclusivamente a aquello que sea estrictamente necesario y que las medidas de seguridad serán proporcionales a los intereses que sea preciso proteger y a los riesgos reales o potenciales en torno a esos intereses, permitiendo una defensa de los mismos que cause el mínimo trastorno posible.

3. Fundamentos de la seguridad de la información

Los fundamentos de una seguridad de la información óptima son los siguientes:

a) en el Parlamento Europeo, un servicio de garantía de la seguridad de la información (INFOSEC), responsable de colaborar con la autoridad de seguridad correspondiente, a fin de facilitar información y prestar asesoramiento sobre las amenazas técnicas para la seguridad y los medios de protección frente a dichas amenazas;

b) una estrecha colaboración entre los servicios competentes del Parlamento Europeo y los servicios de seguridad de las demás instituciones de la UE.

4. Principios relativos a la seguridad de la información

4.1. *Objetivos*

Los objetivos principales de la seguridad de la información son los siguientes:

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

b) proteger la información clasificada de la UE facilitada en las comunicaciones y los sistemas y redes de información frente a las amenazas para su confidencialidad, integridad y disponibilidad;

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

d) en caso de fallo de la seguridad, evaluar el perjuicio causado, limitar sus consecuencias, llevar a cabo investigaciones de seguridad y adoptar las medidas necesarias para remediarlo.

4.2. *Clasificación*

4.2.1. En lo que atañe a la confidencialidad, se requieren cierta cautela y experiencia a la hora de seleccionar la información y el material que vayan a protegerse y evaluar el grado de protección requerido. Resulta fundamental que el grado de protección se corresponda con la importancia que revista, desde el punto de vista de la seguridad, el elemento concreto de información o el material que haya de protegerse. A fin de garantizar que la información circule adecuadamente, se evitará una clasificación superior o inferior a la requerida.

4.2.2. El sistema de clasificación es el instrumento que permite aplicar los principios establecidos en la presente sección; deberá aplicarse un sistema de clasificación similar a efectos de la planificación y organización de los medios necesarios para luchar contra el espionaje, el sabotaje, el terrorismo y otras amenazas, de tal modo que se proporcione la máxima protección a los locales más importantes donde se encuentre información clasificada de la UE y de los puntos más sensibles de dichos locales.

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

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

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

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

4.3. *Objetivos de las medidas de seguridad*

Las medidas de seguridad deberán:

a) aplicarse a todas las personas que tengan acceso a información clasificada de la UE, a los soportes de la información clasificada de la UE y a otra información confidencial, así como 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 posición pueda poner en peligro la seguridad de dicha información y de instalaciones importantes en que se encuentre dicha información, y proceder a su exclusión o traslado;

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

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

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

5. **Normas mínimas comunes**

El Parlamento garantizará la observancia de normas mínimas comunes de seguridad por parte de todos los destinatarios de información clasificada de la UE tanto dentro de la institución como bajo su competencia, a saber, los servicios y contratistas, de tal modo que exista la certeza, al comunicarse dicha información, de que vaya a ser tratada con igual cautela. Estas normas mínimas incluirán criterios para la habilitación de seguridad de funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos, y procedimientos para la protección de la información confidencial.

El Parlamento Europeo autorizará el acceso a dicha información a órganos externos únicamente si estos garantizan que, este tipo de información se tratará de conformidad con disposiciones que sean al menos estrictamente equivalentes a dichas normas mínimas comunes.

Estas normas mínimas comunes se aplicarán también cuando el Parlamento Europeo confíe, mediante contrato o convenio de subvención, a entidades industriales o de otra índole tareas que conlleven, impliquen o incluyan información confidencial.

6. **Seguridad para los funcionarios del Parlamento Europeo y otros empleados del parlamento que trabajen para los grupos políticos**

6.1. *Instrucciones en materia de seguridad para los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos*

Los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos que ocupen puestos en los que puedan tener acceso a información clasificada de la UE recibirán, en el momento de asumir sus funciones y a intervalos regulares posteriormente, instrucciones completas sobre la necesidad de la seguridad y los procedimientos para conseguirla. Deberá exigirse a estas personas que certifiquen por escrito que han leído y comprendido perfectamente las disposiciones en materia de seguridad aplicables.

6.2. *Responsabilidades de gestión*

El personal de dirección tendrá la obligación de saber quiénes son los miembros de su personal que trabajan con información clasificada o tienen acceso a sistemas de comunicación e información de seguridad, así como la obligación de registrar y comunicar todo incidente o aparente muestra de vulnerabilidad que puedan afectar a la seguridad.

6.3. *Estatuto de seguridad de los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos*

Deberán establecerse los procedimientos necesarios para garantizar que, cuando se den a conocer informaciones negativas sobre un funcionario del Parlamento Europeo u otro empleado del Parlamento que trabaje para un grupo político, se determine si esta persona trabaja con información clasificada o tiene acceso a sistemas de comunicación o información de seguridad, y se informe a los servicios competentes del Parlamento Europeo. En caso de que se determine que representa un riesgo para la seguridad, dicha persona será excluida o cesada en las funciones en que pueda poner en peligro la seguridad.

7. **Seguridad física**

Por «seguridad física» se entiende la aplicación de medidas de protección física y técnica para impedir el acceso no autorizado a información clasificada de la UE.

7.1. *Necesidad de protección*

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

7.2. *Verificación*

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.

7.3. *Seguridad de los edificios*

Los edificios en que se encuentren información clasificada de la UE o sistemas de comunicación e información de seguridad deberán estar protegidos contra el acceso no autorizado.

El tipo de protección proporcionado a la información clasificada de la UE, por ejemplo, bloqueo de ventanas, cerraduras en las puertas, guardias en las entradas, sistemas automatizados de control de acceso, controles y patrullas de seguridad, sistemas de alarma, sistemas de detección de intrusos y perros de vigilancia, dependerá de:

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

b) la calidad de los muebles de seguridad destinados a la información y el material de que se trate; y

c) la naturaleza física y la ubicación del edificio.

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

7.4. *Planes de contingencia*

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

8. **Indicaciones de seguridad, marcados, estampación y gestión de la clasificación**

8.1. *Indicaciones de seguridad*

No están permitidas otras clasificaciones que las definidas en el artículo 2, letra c) de la presente Decisión.

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

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

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

8.2. *Marcados*

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

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

8.3. *Estampación de la clasificación*

La clasificación se estampará del siguiente modo:

a) en los documentos clasificados como «RESTREINT UE/EU RESTRICTED», por medios mecánicos o electrónicos;

b) en los documentos clasificados como «CONFIDENTIEL UE/EU CONFIDENTIAL», por medios mecánicos, a mano o mediante impresión en papel preestampillado y registrado;

c) en los documentos clasificados como «SECRET UE/EU SECRET» y «TRÈS SECRET UE/EU TOP SECRET», por medios mecánicos o a mano.

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

8.4. *Gestión de la clasificación*

8.4.1. Aspectos generales

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

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

Los funcionarios del Parlamento Europeo clasificarán, recalificarán o desclasificarán la información siguiendo instrucciones o por delegación del Secretario General.

Los procedimientos precisos para el tratamiento de los documentos clasificados se concebirán para garantizar la protección adecuada de la información que contengan.

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 el SIC.

8.4.2. Aplicación de la clasificación

La clasificación de un documento se determinará con arreglo al nivel de sensibilidad de su contenido, de acuerdo con las definiciones del artículo 2, letra c). 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».

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

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

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

9. **Inspecciones**

La Dirección responsable de la Seguridad del Parlamento Europeo, que podrá estar asistida por el SIC, llevará a cabo inspecciones periódicas de las disposiciones de seguridad para la protección de la información clasificada de la UE.

La Dirección de responsable de la Seguridad del Parlamento Europeo y los servicios de seguridad de otras instituciones, órganos y organismos establecidos virtud o sobre la base de los Tratados que traten información clasificada de la UE podrán acordar también la realización de evaluaciones inter pares de las disposiciones de seguridad para la protección de la información clasificada de la UE.

10. **Procedimiento de desclasificación**

10.1. El SIC examinará la información clasificada de la UE y formulará propuestas de desclasificación al autor de un documento, como máximo 25 años después de la fecha de su creación. Los documentos no desclasificados en un primer examen se reexaminarán periódicamente y al menos cada cinco años.

10.2. Además de los documentos conservados en los archivos seguros y adecuadamente clasificados, el proceso de desclasificación puede abarcar también otra información confidencial existente en los archivos seguros o el Centro de Archivo y Documentación del Parlamento Europeo (CARDOC).

10.3. En nombre del autor, el SIC se encargará de informar de la modificación en la clasificación a los destinatarios del documento; estos, por su parte, se encargarán de informar de dicha modificación a los destinatarios subsiguientes a quienes hayan enviado el documento o una copia del mismo.

10.4. La desclasificación no afectará a ningún marcado que pueda aparecer en el documento.

10.5. La clasificación original en la cabecera y al pie de cada página deberá tacharse. La primera página (portada) del documento deberá sellarse y completarse con la referencia del SIC.

10.6. El texto del documento desclasificado deberá adjuntarse a la ficha electrónica o sistema equivalente en que se haya registrado.

10.7. En el caso de los documentos cubiertos por la excepción relativa a la intimidad y a la integridad las personas o a los intereses comerciales de una persona física o jurídica, así como en el caso de los documentos sensibles, se aplicará el artículo 2 del Reglamento(CEE, Euratom) nº 354/83.

10.8. Además de las disposiciones de los puntos 10.1. a 10.7 se aplicarán las normas siguientes:

a) en el caso de documentos de terceros, el SIC consultará a los terceros implicados antes de proceder a la desclasificación; los terceros dispondrán de ocho semanas para presentar observaciones;

b) en lo referente a la excepción relativa a la intimidad y la integridad de las personas, en el proceso de desclasificación se tendrá en cuenta, en particular, el acuerdo de la persona afectada, la imposibilidad de identificar a la persona afectada y el hecho de que esa persona ya haya fallecido;

c) en lo referente a la excepción relativa a los intereses comerciales de una persona física o jurídica, podrá notificarse a la persona afectada mediante publicación en el *Diario Oficial de la Unión Europea* y darle un plazo de cuatro semanas desde el día de la publicación para formular posibles observaciones.

PARTE 2

PROCEDIMIENTO DE HABILITACIÓN DE SEGURIDAD

11. **Procedimiento de habilitación de seguridad para los diputados al Parlamento Europeo**

11.1. A la vista de las prerrogativas y competencias del Parlamento Europeo, a sus diputados se les podrá conceder acceso a la información clasificada de la UE hasta el nivel «CONFIDENTIEL UE/EU CONFIDENTIAL» incluido sin habilitación de seguridad. Para acceder a la información clasificada como 'CONFIDENTIEL UE/EU CONFIDENTIAL' deberán firmar una declaración solemne de no divulgarán el contenido de dicha información a terceros.

11.2. Para acceder a información clasificada como «TRÈS SECRET UE/EU TOP SECRET» y «SECRET UE/EU SECRET», los diputados al Parlamento Europeo deberán haber sido autorizados para ello con arreglo al procedimiento previsto en los puntos 11.3 y 11.4.

11.3. Sólo se concederá la autorización a los diputados al Parlamento Europeo que hayan sido sometidos a una comprobación de seguridad por las autoridades nacionales competentes de los Estados miembros conforme al procedimiento previsto en los puntos 11.9. a 11.14. El Presidente será responsable de la concesión de autorización a los diputados.

11.4. El Presidente podrá conceder 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 puntos 11.8. a 11.13.

11.5. La Dirección responsable de la Seguridad del Parlamento Europeo llevará una lista actualizada de todos los diputados al Parlamento Europeo que hayan recibido una autorización, también en caso de que ésta sea provisional en el sentido del punto 11.15.

11.6. La autorización será válida durante un período de cinco años o mientras duren las tareas que motivaron su concesión, si su duración es inferior. Podrá ser renovada de acuerdo con el procedimiento establecido en el punto 11.4.

11.7. El Presidente retirará la autorización si considera que hay motivos que lo justifican. Toda decisión de retirar la autorización se notificará al diputado al Parlamento Europeo interesado, que podrá solicitar ser oído por el Presidente antes de que surta efecto la retirada, y a la autoridad nacional competente.

11.8. La comprobación de seguridad se realizará con la asistencia del diputado al Parlamento Europeo interesado y a instancias del Presidente. La autoridad nacional competente para realizar la comprobación de seguridad será la del Estado miembro del que sea nacional el diputado interesado.

11.9. En el marco del procedimiento de comprobación de seguridad, se solicitará al diputado al Parlamento Europeo interesado que rellene una ficha personal de información.

11.10. El Presidente especificará en su solicitud a las autoridades nacionales competentes el nivel de información clasificada que se pondrá a disposición del diputado al Parlamento Europeo interesado, de manera que aquellas puedan llevar a cabo la comprobación de seguridad.

11.11. El conjunto del procedimiento de comprobación de seguridad realizado por las autoridades nacionales, junto con los resultados obtenidos, se ajustará a la normativa pertinente en vigor en el Estado miembro interesado, incluida la relativa a los recursos.

11.12. En caso de que las autoridades nacionales competentes del Estado miembro emitan un dictamen positivo, el Presidente podrá conceder la autorización al diputado al Parlamento Europeo interesado.

11.13. De emitirse un dictamen negativo de las autoridades nacionales competentes, dicho dictamen se notificará al diputado al Parlamento Europeo interesado, que podrá solicitar ser oído por el Presidente. Si lo considera necesario, el Presidente podrá solicitar a las autoridades nacionales competentes cualquier otra aclaración. En caso de que se confirme el dictamen negativo, no se concederá la autorización.

11.14. Todos los diputados al Parlamento Europeo a los que se conceda autorización con arreglo al punto 11.3. recibirán, en el momento en que se conceda la autorización y a intervalos regulares posteriormente, las directrices necesarias sobre la protección de la información clasificada y sobre los medios para garantizar dicha protección. Dichos diputados firmarán una declaración en la que harán constar que han recibido dichas directrices.

11.15. En circunstancias excepcionales, el Presidente podrá, previa notificación a las autoridades nacionales competentes y siempre que estas no respondan en el plazo de un mes, conceder a un diputado al Parlamento Europeo una autorización provisional para un período no superior a seis meses, en espera del resultado de la comprobación de seguridad prevista en el punto 11.11. Las autorizaciones provisionales concedidas de esta forma no darán acceso a la información clasificada como «TRÈS SECRET UE / EU TOP SECRET».

12. **Procedimiento de habilitación de seguridad de funcionarios del Parlamento y otros empleados del parlamento que trabajen para los grupos políticos**

12.1. Sólo podrán tener acceso a la información clasificada los funcionarios del Parlamento Europeo y otros empleados del Parlamento que trabajen para los grupos políticos que, por sus tareas y por necesidades del servicio, deban tener conocimiento de dicha información o utilizarla.

12.2. Para tener acceso a información clasificada como «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET» y «CONFIDENTIEL UE/EU CONFIDENTIAL», las personas mencionadas en el punto 12.1. deberán haber sido autorizadas para ello con arreglo al procedimiento previsto en los puntos 12.3.y 12.4.

12.3. Sólo se concederá la autorización a las personas a que se refiere el punto 12.1. que hayan sido sometidas a una comprobación de seguridad por las autoridades nacionales competentes de los Estados miembros conforme al procedimiento previsto en los puntos 12.9. a 12.14. El Secretario General será responsable de la concesión de autorización a los funcionarios del Parlamento Europeo y los empleados del Parlamento que trabajen para los grupos políticos.

12.4. El Secretario General podrá conceder 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 puntos 12.8. a 12.13.

12.5. La Dirección responsable de la Seguridad del Parlamento Europeo llevará una lista actualizada de todos los puestos que requieran una habilitación de seguridad, comunicados por los correspondientes servicios del Parlamento Europeo, y de todas las personas que hayan recibido una autorización, también en caso de que ésta sea provisional en el sentido del punto 12.15.

12.6. La autorización, será válida durante un período de cinco años o mientras duren las tareas que motivaron su concesión, si su duración es inferior. Podrá ser renovada de acuerdo con el procedimiento establecido en el punto 12.4.

12.7. El Secretario General retirará la autorización si considera que hay motivos que lo justifican. La decisión de retirar la autorización se notificará al funcionario del Parlamento Europeo o empleado del Parlamento que trabaje para los grupos políticos interesado, que podrá solicitar ser oído por el Secretario General antes de que surta efecto la retirada, y a la autoridad nacional competente.

12.8. La comprobación de seguridad se realizará con la asistencia de la persona interesada y a instancias del Secretario General. La autoridad nacional competente será la del Estado miembro del que sea nacional la persona interesada. Cuando lo permitan las disposiciones legales y reglamentarias nacionales, las autoridades nacionales competentes podrán realizar investigaciones sobre no nacionales que requieran acceso a información clasificada como «CONFIDENTIEL UE/EU CONFIDENTIAL» o superior.

12.9. En el marco del procedimiento de comprobación de seguridad, se solicitará al funcionario del Parlamento Europeo o empleado del Parlamento que trabaje para los grupos políticos interesado que rellene una ficha personal de información.

12.10. El Secretario General especificará en su solicitud a las autoridades nacionales competentes el tipo y el nivel de información clasificada que se pondrá a disposición de la persona interesada, de manera que aquellas puedan llevar a cabo la comprobación de seguridad y dar su opinión sobre el nivel de autorización que sería adecuado conceder a dicha persona.

12.11. El conjunto del procedimiento de comprobación de seguridad realizado por las autoridades nacionales, con los resultados obtenidos, se regirá por la normativa pertinente en vigor en el Estado miembro interesado, incluida la relativa a los recursos.

12.12. En caso de que las autoridades nacionales competentes del Estado miembro emitan un dictamen positivo, el Secretario General podrá conceder la autorización a la persona interesada.

12.13. De emitirse un dictamen negativo de las autoridades nacionales competentes, dicho dictamen se notificará al funcionario del Parlamento Europeo o empleado del Parlamento que trabaje para los grupos políticos interesado, que podrá solicitar ser oído por el Secretario General. Si lo considera necesario, el Secretario General podrá solicitar a las autoridades nacionales competentes cualquier otra aclaración. En caso de que se confirme el dictamen negativo, no se concederá la autorización.

12.14. Todos los funcionarios del Parlamento Europeo y empleados del Parlamento que trabajen para los grupos políticos a los que se conceda autorización con arreglo a los puntos 12.14. y 12.15. 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. Dichos funcionarios del Parlamento Europeo y empleados del Parlamento que trabajen para los grupos políticos firmarán una declaración en la que harán constar que han recibido las instrucciones y se comprometerán a acatarlas.

12.15. En circunstancias excepcionales, el Secretario General podrá, previa notificación a las autoridades nacionales competentes y siempre que estas no respondan en el plazo de un mes, conceder a un funcionario del Parlamento Europeo o empleado del Parlamento que trabaje para los grupos políticos una autorización provisional para un período no superior a seis meses, en espera del resultado de la comprobación de seguridad prevista en el punto 12.11. Las autorizaciones provisionales concedidas de esta forma no darán acceso a la información clasificada como 'TRÈS SECRET UE/EU TOP SECRET'.