2024/1418

24.5.2024

Decisión Delegada n.º 19/2024 sobre las normas de desarrollo para el manejo de información CONFIDENTIEL UE/EUCONFIDENTIAL y SECRET UE/EU SECRET

EL COMITÉ ADMINISTRATIVO DEL TRIBUNAL DE CUENTAS EUROPEO,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular su artículo 287,

Vista la Decisión n.º 41/2021 del Tribunal de Cuentas, sobre las normas de seguridad para la protección de la información clasificada de la UE (ICUE) ([1]), en lo sucesivo, la «Decisión n.º 41-2021»,

Vista la política de seguridad de la información del Tribunal de Cuentas (actualmente DEC 127/15 FINAL) y la política de clasificación de información (Circular n.º 123/20) ([2]),

Vistos los debates mantenidos por el Comité Administrativo en su reunión del día 18 de marzo de 2024,

Considerando que la Decisión n.º 41-2021 se aplica a todos los servicios y en todos los locales del Tribunal de Cuentas,

Considerando que el artículo 1, apartado 3, de la Decisión n.º 41-2021 dispone que se adoptarán medidas para que el personal del Tribunal de Cuentas que necesite acceder a grados superiores de ICUE lo haga en locales adecuados de otras instituciones, órganos y organismos de la UE,

Considerando que el artículo 1, apartado 3, y el artículo 5, apartado 6, de la Decisión n.º 41-2021 dispone que el Tribunal de Cuentas podrá suscribir un acuerdo con otra institución de la UE en Luxemburgo para poder manejar y almacenar información CONFIDENTIEL UE/EU CONFIDENTIAL o superior en una zona de acceso restringido de dicha institución, y que se firmó un memorando de entendimiento con la Dirección General de Recursos Humanos y Seguridad de la Comisión el 25 de septiembre de 2023 sobre la utilización de la zona de acceso restringido de la dirección de seguridad en Luxemburgo,

Considerando que las medidas de seguridad para proteger la información clasificada de la UE (ICUE) a lo largo de su ciclo de vida deben ser acordes, en particular, con su clasificación de seguridad,

Considerando que las medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de información comunicada al Tribunal de Cuentas serán adecuadas a la naturaleza y el tipo de la información de que se trate,

Considerando que el artículo 3, apartado 3, de la Decisión n.º 41-2021 exige que la ICUE esté protegida por medidas de seguridad físicas, y la información clasificada con grado CONFIDENTIEL UE/CONFIDENTIAL EU o superior se protegerá además con medidas de seguridad de personal,

Considerando que el artículo 10, apartado 10, de la Decisión n.º 41-2021 dispone que el Comité Administrativo adoptará una decisión delegada por la que se establecen normas de aplicación; de conformidad con los artículos 8, apartado 1, y 10, apartado 1, de la Decisión n.º 41-2021 estas regularán cuestiones como el manejo y almacenamiento de ICUE, así como fallos de seguridad,

Considerando que el Tribunal de Cuentas aseguró, mediante la Decisión n.º 41-2021, que sus medidas de seguridad para garantizar un alto nivel de protección de la ICUE son equivalentes a las establecidas por la normativa aplicable en otras instituciones, agencias y organismos de la UE en materia de protección de la ICUE;

Considerando un acuerdo administrativo entre el Tribunal de Cuentas y la Comisión, el Consejo y el SEAE que entró en vigor el 27 de enero de 2023,

([1]) DO L 256 de 19.7.2021, p. 106.
([2]) Puede consultarse en https://www.eca.europa.eu/es/legal-framework.

DECIDE:

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Decisión establece las condiciones para el manejo de información clasificada de la UE (ICUE) CONFIDENTIEL UE/EU CONFIDENTIAL ([3]) y SECRET UE/EU SECRET ([4]) de conformidad con la Decisión n.º 41/2021 del Tribunal de Cuentas.

2. La presente Decisión se aplicará a todos los servicios del Tribunal de Cuentas y en todos sus locales. También se aplicará a sus Salas y Comités, que se incluyen en el término «servicios» a efectos de la presente Decisión.

Artículo 2

Criterios de acceso a la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. El acceso a la información clasificada como CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET podrá concederse después de que:

a) se haya determinado la necesidad de que un particular tenga acceso a determinada información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET a fin de poder desempeñar una función o cometido profesional para el Tribunal de Cuentas;

b) esa persona haya sido instruida acerca de las normas y los niveles de seguridad pertinentes y de las directrices para la protección de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET;

c) dicha persona haya asumido sus responsabilidades por escrito en materia de protección de dicha información, y

d) dicha persona haya obtenido una habilitación de seguridad y recibido autorización de acceso por parte del Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas hasta el grado pertinente y una fecha especificada, conforme al artículo 4, apartado 4, de la Decisión n.º 41/2021.

2. No se asignará a los trabajadores en prácticas del Tribunal de Cuentas tareas que requieran acceso a información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

3. El acceso a esa información por parte de otras categorías de personal se autorizará o denegará de acuerdo con el cuadro que figura en el anexo.

([3]) Con arreglo al artículo 1, apartado 2, letra a), de la Decisión n.º 41/2021, por información CONFIDENTIEL UE/EU CONFIDENTIAL se entenderá «información y material cuya revelación no autorizada pueda causar perjuicio a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros».

([4]) Con arreglo al artículo 1, apartado 2, letra a), de la Decisión n.º 41/2021, por información SECRET UE/EU SECRET se entenderá «información y material cuya revelación no autorizada pueda causar un perjuicio grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros».

CAPÍTULO 2

CREACIÓN DE INFORMACIÓN CONFIDENTIEL UE/EU CONFIDENTIAL Y SECRET UE/EU SECRET

Artículo 3

Originador

Si bien el originador en el sentido del artículo 2, letra m), de la Decisión n.º 41/2021 es la institución, agencia u organismo de la Unión Europea, Estado miembro, tercer Estado u organización internacional bajo cuya autoridad se haya producido información clasificada o se haya introducido en las estructuras de la Unión, el redactor de la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET no ha de ser necesariamente la misma entidad.

Artículo 4

Asignación del grado de clasificación

1. Los documentos deberán clasificarse, como mínimo, con el grado CONFIDENTIEL UE/EU CONFIDENTIAL si su revelación no autorizada pudiera, entre otros supuestos:

a) dañar gravemente las relaciones diplomáticas, como ocasionar protestas formales u otras sanciones;

b) perjudicar la seguridad o libertad individuales;

c) perjudicar la eficacia o seguridad operativa del personal desplegado de los Estados miembros o de otros contribuyentes, o la eficacia de importantes operaciones de seguridad o inteligencia;

d) menoscabar sustancialmente la viabilidad financiera de organizaciones importantes;

e) entorpecer la investigación de algún delito grave o facilitarlo;

f) menoscabar notablemente los intereses financieros, monetarios, económicos y comerciales de la Unión o de sus Estados miembros;

g) poner graves obstáculos al desarrollo o al funcionamiento de políticas prioritarias de la UE;

h) interrumpir o perturbar notablemente actividades importantes de la UE;

i) conducir al descubrimiento de información clasificada en un grado superior.

2. La información deberá clasificarse, como mínimo, con el grado SECRET UE/EU SECRET si su revelación no autorizada pudiera, entre otros supuestos:

a) crear tensiones internacionales;

b) deteriorar gravemente las relaciones con países terceros u organizaciones internacionales;

c) poner en peligro directamente la vida o dañar gravemente el orden público o la seguridad o libertad individuales;

d) perjudicar gravemente la eficacia o la seguridad operativa del personal desplegado de los Estados miembros o de otros contribuyentes o el mantenimiento de la eficacia de operaciones de seguridad o inteligencia de gran importancia;

e) perjudicar gravemente los intereses financieros, monetarios, económicos o comerciales de la Unión o de sus Estados miembros;

f) conducir al descubrimiento de información clasificada en un grado superior.

3. Los originadores podrán optar por atribuir un grado de clasificación estándar a determinadas categorías de información que creen de forma habitual. No obstante, se asegurarán de que se atribuye el grado de clasificación apropiado a las informaciones concretas

Artículo 5

Tratamiento de los borradores

1. La información se clasificará tan pronto como se haya producido. Las notas personales, los borradores o los mensajes que contengan información que justifique una clasificación CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET estarán marcados consiguientemente desde el principio y se producirán y manejarán conforme a lo dispuesto en la presente Decisión.

2. Si el documento final deja de justificar la clasificación inicial, se rebajará de grado o se desclasificará, previa confirmación del originador del documento de que es seguro proceder de tal forma.

Artículo 6

Registro del material original

Para permitir el ejercicio del control de originador, de conformidad con el artículo 14, los originadores de documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET deberán, en la medida de lo posible, mantener un registro de todas las fuentes clasificadas que hayan utilizado para producir documentos clasificados, incluidos los datos de las fuentes originarias de los Estados miembros de la UE, organizaciones internacionales o terceros países. Cuando así proceda, la información clasificada agregada se marcará de una forma que preserve la identificación de los originadores de los materiales originales clasificados que se hayan utilizado.

Artículo 7

Clasificación de partes de un documento

1. De conformidad con el apartado 12 de la política de clasificación de la información del Tribunal de Cuentas, el grado global de clasificación de un documento deberá ser al menos igual al de su componente con mayor grado de clasificación. Cuando se recopile información procedente de diversas fuentes, se revisará el documento agregado final para determinar su grado global de clasificación de seguridad, al ser posible que requiera un grado de clasificación superior al de sus componentes.

2. Los documentos que contengan partes clasificadas y partes no clasificadas se estructurarán y marcarán de forma que los componentes con distintos grados de clasificación o sensibilidad puedan identificarse fácilmente y separarse en caso necesario. De esta forma, cada una de las partes podrá manejarse adecuadamente cuando se separe de los demás componentes.

Artículo 8

Marca de clasificación completa

1. La información cuya clasificación esté justificada se marcará y manejará como tal, con independencia de su forma física. El grado de clasificación se comunicará claramente a los destinatarios, bien mediante una marca de clasificación, si la información se facilita por escrito —ya sea en papel, en soportes de almacenamiento extraíbles o en un sistema de información y comunicación (SIC)—, bien mediante una notificación, si la información se presenta oralmente (por ejemplo, en una conversación o una presentación). El material clasificado estará marcado físicamente para permitir la fácil identificación de su clasificación de seguridad.

2. En los documentos, se escribirá la marca de clasificación completa CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en letras mayúsculas, en francés y en inglés (primero en francés), de conformidad con el apartado 3. Esta marca no se traducirá a otras lenguas.

3. La marca de clasificación CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se dispondrá de la forma siguiente:

a) centrada en la parte superior e inferior de cada página del documento;

b) la marca de clasificación completa aparecerá en una sola línea, sin espacios a cada lado de la barra oblicua;

c) en mayúsculas de color negro, con el tipo y tamaño de letra Times New Roman 16 (dentro de lo posible, pero al menos 14), en negrita y rodeada de un reborde por cada lado.

4. Si se crea un documento con información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET:

a) se marcará claramente cada página con el grado de clasificación;

b) se numerarán todas las páginas;

c) el documento deberá llevar un número de referencia, un número de registro y una indicación del asunto, que en sí misma no constituirá información clasificada, salvo si se marca como tal;

d) todos los anexos y documentos adjuntos se enumerarán, siempre que sea posible, en la primera página, y

e) se indicará la fecha de creación en el documento.

5. En la medida de lo posible, la marca de SECRET UE/EU SECRET figurará en rojo.

Artículo 9

Marcas abreviadas de clasificación C-UE/EU-C y S-EU/EU-S

Podrán utilizarse las abreviaturas «C-UE/EU-C» y «S-UE/EU-S» para indicar el grado de clasificación de partes concretas de un documento con información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, o cuando no pueda insertarse la marca de clasificación completa, por ejemplo, en un pequeño soporte de almacenamiento extraíble. Podrá también utilizarse en el cuerpo del texto cuando resulte oneroso el uso repetido de las marcas de clasificación completa. La abreviatura no se utilizará en lugar de las marcas de clasificación completas que han de figurar en el encabezamiento y el pie de página del documento.

Artículo 10

Otros indicadores de seguridad

1. Los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrán llevar otras marcas o «indicadores de seguridad» que especifiquen, por ejemplo, el ámbito al que pertenece el documento o que indiquen una distribución determinada en función de la «necesidad de conocer». Por ejemplo:

DIVULGABLE A LIECHTENSTEIN

2. Los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrán llevar una advertencia de seguridad con instrucciones específicas para la gestión y el manejo de los documentos.

Siempre que sea posible, toda indicación referente a la desclasificación se colocará en la primera página del documento en el momento de su creación. Por ejemplo, podrá utilizarse el marcado siguiente:

SECRET UE/EU SECRET hasta el [dd.mm.aaaa] y RESTREINT UE/ EU RESTRICTED posteriormente

Artículo 11

Tratamiento electrónico

1. Los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se crearán por medios electrónicos siempre que estos estén disponibles.

2. Si se genera información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el personal del Tribunal de Cuentas empleará un SIC acreditado al menos en el correspondiente grado de clasificación. En caso de duda, debería solicitarse asesoramiento del Responsable de seguridad de la información del Tribunal de Cuentas.

3. Los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, incluidos los borradores (véase el artículo 5), no deberán remitirse por correo electrónico, ni se imprimirán o escanearán en impresoras o escáneres estándar, ni se manejarán en los dispositivos personales de los miembros del personal. Solo podrá emplearse, a fin de imprimir documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, impresoras o fotocopiadoras conectadas a ordenadores independientes protegidos de emisiones electromagnéticas o a un sistema acreditado.

Artículo 12

Registro a efectos de seguridad

1. La información clasificada como CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se inscribirá en un registro para fines de seguridad antes de ser distribuida y al ser recibida. Se registrará:

— a su entrada en la zona de acceso restringido de la Comisión en Luxemburgo, o a su salida de esta, para cuyo uso el Tribunal de Cuentas ha celebrado un memorando de entendimiento, y

— cuando llegue a un SIC o salga de él.

2. Esta información podrá registrarse en papel o en libros de registro electrónicos.

3. Si la información se maneja por vía electrónica en un SIC, el registró podrá también realizarse mediante procesos internos del SIC. En dicho supuesto, el SIC deberá incluir medidas para garantizar la integridad de los registros.

4. El controlador del registro mantendrá un registro que contenga, al menos, la siguiente información en cada documento:

a) la fecha de registro del documento final clasificado;

b) el nivel de clasificación;

c) si procede, la fecha de expiración del grado de clasificación;

d) la denominación del servicio originario;

e) los destinatarios;

f) el objeto;

g) el número de referencia para el documento del servicio originario;

h) el número de registro;

i) el número de copias distribuidas;

j) en la medida de lo posible, el registro de fuentes empleadas para crear el documento;

k) la fecha de degradación o desclasificación del documento, y

l) los detalles referentes a la destrucción (lugar, fecha, método, supervisión y certificado de destrucción).

Artículo 13

Distribución

El remitente de los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET decidirá a quién debe distribuirse la información, en función de su «necesidad de conocer». Deberá elaborarse una lista de distribución para garantizar que se aplica correctamente el principio de la «necesidad de conocer».

CAPÍTULO 3

TRABAJO CON INFORMACIÓN CONFIDENTIEL UE/EU CONFIDENTIAL Y SECRET UE/EU SECRET EXISTENTE

Artículo 14

Control de originador

1. El originador deberá tener «control de originador» sobre la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET que haya creado. Se recabará el consentimiento previo por escrito del originador antes de que la información pueda ser:

a) desclasificada u objeto de una rebaja del nivel de clasificación;

b) utilizada con fines distintos de los determinados por el originador;

c) divulgada a un tercer país o a una organización internacional; o

d) revelada a una parte externa al Tribunal de Cuentas pero dentro de la UE.

2. Los poseedores de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET serán personas debidamente autorizadas que han recibido acceso a la información clasificada para poder desempeñar sus funciones. Son responsables de su correcto manejo, almacenamiento y protección de dicha información con arreglo a la Decisión n.º 41/2021. A diferencia de los originadores de información clasificada, los poseedores no estarán autorizados para adoptar decisiones sobre la degradación, desclasificación o la subsiguiente divulgación de información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

3. Si no es posible identificar al originador de información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el servicio del Tribunal de Cuentas que posea la información clasificada ejercerá el control de originador. Si el poseedor considera necesario divulgar información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET a un tercer país o a una organización internacional, el Tribunal de Cuentas consultará a una de las partes de un acuerdo de seguridad de la información celebrado con ese mismo tercer país u organización internacional ([5]).

Artículo 15

SIC adecuado para manejar información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

La información con grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se manejará y transmitirá por vía electrónica, en la medida de lo posible. De conformidad con el artículo 6 de la Decisión n.º 41-2021, solo podrán emplearse los SIC y equipos que hayan sido acreditados por otra institución, órgano u organismo de la UE o por el Tribunal de Cuentas para dicho cometido.

Artículo 16

Medidas específicas aplicables a la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET en soportes de almacenamiento extraíbles

1. La utilización de soportes de almacenamiento extraíbles, como llaves USB, CD, DVD o tarjetas de memoria (incluidas tarjetas SSD ([6])) será objeto de control y dará lugar a la debida rendición de cuentas. Solo podrán utilizarse soportes de almacenamiento extraíbles proporcionados por el Tribunal de Cuentas o por otra institución, agencia u organismo de la UE, aprobados por el responsable de seguridad de la información y cifrados con un producto aprobado por dicho responsable. No deberán utilizarse soportes de almacenamiento extraíbles personales ni soportes distribuidos gratuitamente en conferencias, seminarios, etc., para transmitir información clasificada. Con arreglo a las orientaciones del responsable de seguridad de la información, siempre que fuera posible deberían emplearse los soportes de almacenamiento extraíble protegidos por la tecnología Tempest.

([5]) Véase el artículo 35 para obtener más información.

([6]) SSD se refiere a un dispositivo de almacenamiento por semiconductores, un dispositivo o una unidad de estado sólido.

2. Cuando un documento clasificado se maneje o se almacene electrónicamente en soportes de almacenamiento extraíbles, como llaves USB, discos compactos o tarjetas de memoria, la marca de clasificación deberá ser claramente visible en la propia información, así como en el nombre del archivo y en el soporte de almacenamiento extraíble.

3. El personal deberá tener en cuenta que, cuando se almacenen grandes volúmenes de información clasificada en soportes de almacenamiento extraíbles, los dispositivos podrán requerir un grado de clasificación más elevado.

4. Podrán utilizarse solamente los SIC acreditados para transmitir información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET hacia o desde soportes de almacenamiento extraíbles.

5. Antes de descargar dicha información a un soporte de almacenamiento extraíble, se tomarán especiales precauciones para asegurar que dichos soportes no contengan virus o programas maliciosos.

6. Cuando así proceda, los soportes de almacenamiento extraíbles se tratarán con arreglo a los procedimientos operativos de seguridad correspondientes al sistema de cifrado utilizado.

7. Los documentos en soportes de almacenamiento extraíbles que ya no se necesiten o que hayan sido transferidos a un SIC adecuado se suprimirán o eliminarán de forma segura utilizando productos o métodos aprobados. Salvo si se guardan en una caja fuerte adecuada, los soportes de almacenamiento extraíbles se destruirán cuando dejen de ser necesarios. Las operaciones de destrucción o eliminación se efectuarán con métodos que se ajusten a las normas de seguridad del Tribunal de Cuentas. Se mantendrá un inventario de los soportes extraíbles, cuya destrucción deberá registrarse.

Artículo 17

Manejo y almacenamiento de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. De conformidad con el artículo 5, apartados 5 y 6, de la Decisión n.º 41-2021, la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET será tratada en una zona de acceso restringido ([7]). El Tribunal de Cuentas podrá también acceder a esta información en zonas de acceso restringido de otra institución de la UE.

2. Con arreglo al artículo 5, apartado 6, de la Decisión n.º 41-2021, y previo acuerdo del originador, dicha información podrá tratarse a título excepcional en la zona administrativa ([8]) del Tribunal de Cuentas, siempre que la ICUE esté protegida del acceso de toda persona no autorizada.

3. En momentos de crisis o en el supuesto de urgencia, esta información podrá ser tratada fuera de una zona administrativa o de acceso restringido, siempre que el poseedor haya acordado aplicar medidas compensatorias, que serán como mínimo, las siguientes:

— Los documentos CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET no se leerán en lugares públicos.

— La ICUE permanecerá en todo momento bajo el control personal de su poseedor.

— En el caso de los documentos impresos en papel, el poseedor deberá haber notificado al Registro de la ICUE la circunstancia de que los documentos clasificados están siendo manejados fuera de una zona de acceso restringido y de una zona administrativa.

— Los documentos se guardarán en una caja fuerte apropiada cuando no estén siendo leídos o comentados.

— Las puertas de la sala se cerrarán durante la lectura o el debate del documento.

— No podrán tratarse los detalles del documento por teléfono en una línea no segura, ni por correo electrónico.

— El poseedor no fotocopiará ni escaneará documentos. Únicamente el Registro de la ICUE podrá facilitar copias adicionales.

([7]) Según se define en el artículo 18 de la Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

([8]) Según se define en el anexo de la Decisión n. º 41/2021.

— Los documentos solo podrán tratarse y mantenerse temporalmente fuera de una zona administrativa o de acceso restringido el tiempo que sea absolutamente necesario, y posteriormente serán devueltos al Registro de la ICUE.

— Los documentos deberán ser firmados a su devolución.

— El poseedor no deberá tirar ni destruir documentos clasificados.

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

5. Puede solicitarse asesoramiento adicional al responsable de seguridad de la información.

6. Se informará lo antes posible al responsable de seguridad de la información de todo incidente de seguridad, supuesto o confirmado, que afecte a un documento.

Artículo 18

Copia y traducción de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrá copiarse o traducirse a instrucción de su poseedor, siempre que el originador no haya acordado imponer ninguna reserva al respecto. No obstante, no se realizarán más copias de las estrictamente necesarias. El Tribunal de Cuentas podrá también solicitar al originador que facilite una copia traducida al inglés.

2. Cuando solo se reproduzca parte de un documento clasificado, se aplicarán las mismas condiciones que las relativas al documento íntegro. Los extractos se clasificarán también con el mismo grado, a menos que hayan sido marcados específicamente como no clasificados por el originador.

3. Las medidas de seguridad aplicables a la información original se aplicarán también a sus copias y traducciones.

Artículo 19

Principios generales para llevar información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. En la medida de lo posible, la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET que deba salir de zonas de acceso restringido o de las zonas administrativas, conforme al artículo 17, apartado 2, se enviará por vía electrónica a través de medios debidamente acreditados o protegidos por productos criptográficos aprobados.

2. En función de los medios disponibles y las circunstancias particulares, la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrá llevarse físicamente en mano en papel o en un soporte de almacenamiento extraíble. Para la transmisión de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, el uso de soportes de almacenamiento extraíbles tendrá preferencia sobre el envío de documentos impresos.

3. Conforme al artículo 6, apartado 8, de la Decisión n.º 41-2021, los soportes de almacenamiento extraíbles se encriptarán a través de un producto aprobado para la protección de la ICUE, ya sea por el Consejo o el Secretario General del Consejo en su calidad de autoridad de certificación criptológica, o por otra institución, órgano u organismo de la UE. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET contenida en soportes de almacenamiento extraíbles que no estén protegidos por un producto de cifrado aprobado de esta manera se tratará de la misma manera que la información impresa en papel.

4. Los envíos podrán contener más de un elemento de ICUE, siempre que se respete el principio de la «necesidad de conocer».

5. El envoltorio utilizado deberá garantizar que el contenido está oculto. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se transportará en dos capas de envoltorios opacos, como un sobre, una carpeta opaca o un maletín. El exterior del envoltorio estará sellado y en este no figurará ninguna indicación sobre la naturaleza o el grado de clasificación de su contenido. En la capa interior del envoltorio se marcará CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET. En ambas capas se indicará el nombre del destinatario, su cargo y su dirección, así como una dirección de retorno en caso de que no sea posible efectuar la entrega.

6. El personal o los servicios de mensajería que transporten manualmente la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET recibirán una autorización de seguridad y expedición con certificado de correo.

7. Los sobres y paquetes no deberán abrirse durante el tránsito. La autorización de seguridad expedida a los servicios de mensajería no les otorgará derechos de acceso a la información clasificada en el envío.

8. Conforme al artículo 5, apartado 12, de la Decisión n.º 41/2021, el originador podrá también imponer otras medidas físicas de seguridad con objeto de proteger la información frente a la divulgación no autorizada durante su transporte.

9. Todo incidente de seguridad real o sospechoso con información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET que sea transportada por personal o servicios de mensajería deberá notificarse al responsable de seguridad de la información para que realice una investigación posterior con la menor demora posible.

Artículo 20

Transporte manual de soportes de almacenamiento extraíbles

1. Los soportes de almacenamiento extraíbles que se utilicen para el transporte de información con grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET irán acompañados de una nota de envío en la que se detallarán los soportes de almacenamiento extraíbles y todos los ficheros que alberguen, de forma que el destinatario pueda realizar las comprobaciones necesarias y el acuse de recibo.

2. Los dispositivos solo almacenarán la ICUE que se transporte. Toda la información clasificada contenida en un solo dispositivo deberá tener un único destinatario. Los remitentes deberán tener en cuenta que el almacenamiento de un gran volumen de información clasificada en ese mismo dispositivo podrá justificar la atribución de un grado de clasificación más elevado al dispositivo en su conjunto.

3. Para transportar información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET solo se utilizarán soportes de almacenamiento extraíbles que lleven la marca de clasificación adecuada.

4. Toda información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET guardada en soportes de almacenamiento extraíbles será registrada a efectos de seguridad.

Artículo 21

Transporte de documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET dentro de los departamentos o en las instalaciones del Tribunal de Cuentas

1. El personal que disponga de una autorización de seguridad podrá transportar documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET dentro de los departamentos y en las instalaciones del Tribunal de Cuentas, pero los documentos no podrán ser desatendidos por su portador ni ser leídos en público.

2. Los documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET no serán enviados por correo electrónico interno.

Artículo 22

Transporte de documentos con información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET dentro de la Unión Europea

1. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrá ser transportada por personal o mensajeros del Tribunal de Cuentas o de cualquier otra institución, agencia u organismo de la UE en la que se origine en cualquier lugar de la Unión, siempre que se cumplan las instrucciones siguientes:

a) Se emplearán sobres o envoltorios dobles opacos para transmitir información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET. El exterior del envoltorio estará sellado y en este no figurará ninguna indicación sobre la naturaleza o el grado de clasificación de su contenido.

b) La información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET no deberá ser desatendida por su portador.

c) El sobre o el envoltorio no se deberá abrir en tránsito y la información no deberá leerse en lugares públicos.

2. El personal de la oficina de registro que desee enviar información CONFIDENTIEL UE/EU CONFIDENTIAL a otros lugares de la Unión podrá disponer que se transporte por uno de los medios siguientes:

a) servicios postales nacionales que garanticen un rastreo del envío o servicios de mensajería comercial que garanticen el transporte personal en mano, siempre que cumplan los requisitos establecidos en el artículo 24 de la presente Decisión;

b) valija militar, administrativa o diplomática, en coordinación con el personal de la oficina de registro.

3. El personal que desee remitir información SECRET UE/EU SECRET a otros Estados miembros de la UE solo podrá acordar con el controlador del registro que esta se envíe por valija militar, administrativa o diplomática, y no por servicio postal o de mensajería comercial.

4. Todo el personal del Tribunal de Cuentas o los servicios oficiales de mensajería que porten información CONFIDENTIAL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET llevará un certificado de expedición en cada envío. El controlador del registro deberá expedir el certificado y declarar que el portador está autorizado a realizar el envío.

Artículo 23

Transporte de información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET hacia o desde el territorio de un tercer país

1. La información clasificada con grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET podrá ser transportada en mano por personal del Tribunal de Cuentas o de cualquier otra institución, agencia u organismo de la UE en la que se origine, entre el territorio de la Unión y el territorio de un país tercero.

2. El personal del registro podrá organizar el transporte por valija militar o diplomática.

3. Cuando transporte en mano documentos impresos en papel o soportes de almacenamiento extraíbles clasificados como CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el personal deberá cumplir todas las medidas adicionales siguientes:

— Al desplazarse en transporte público, la información clasificada se colocará en un maletín o bolsa que permanecerá bajo la custodia personal del portador, no pudiendo dejarse en la bodega de equipajes.

— La capa interior del envoltorio deberá llevar un sello oficial que indique que se trata de un envío oficial que no ha de someterse a los controles de seguridad.

— El portador llevará un certificado de correo expedido por el controlador del registro que certifique que está autorizado a transportar el envío CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

Artículo 24

Transporte a cargo de mensajeros comerciales

1. A efectos de lo dispuesto en la presente Decisión, por «mensajeros comerciales» se entienden los servicios postales nacionales y las empresas de mensajería comercial que ofrecen un servicio consistente en la entrega de información a cambio de una tarifa y que se lleva a cabo, bien en forma de transporte personal en mano, bien mediante un sistema de rastreo.

2. Los mensajeros comerciales podrán transportar información CONFIDENTIEL UE/EU CONFIDENTIAL dentro de un mismo Estado miembro de la UE o de un Estado miembro a otro. Los mensajeros comerciales solo podrán transportar información SECRET UE/EU SECRET dentro de un mismo Estado miembro, pero no fuera de su territorio.

3. Los servicios de mensajería comercial recibirán la instrucción de que solo pueden entregar los envíos CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET al controlador del registro, a su sustituto debidamente autorizado o al destinatario previsto.

4. Los servicios de mensajería comercial pueden recurrir a los servicios de un subcontratista. No obstante, la responsabilidad del cumplimiento de la presente Decisión seguirá correspondiendo a la empresa de mensajería.

Artículo 25

Preparación de la ICUE para su trasporte por servicios de mensajería comercial

1. Al preparar envíos clasificados, el remitente deberá tener en cuenta que los servicios de mensajería comercial solo podrán entregar los envíos CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET al controlador del registro, a su sustituto debidamente autorizado o a un destinatario previsto.

2. Cuando se envíe esa información mediante un servicio de mensajería comercial aprobado, el envío se preparará y envolverá de la forma siguiente:

a) El envío se expedirá en doble sobre opaco (las características del sobre interior harán que toda tentativa de abrirlo resulte evidente) u otro material para envoltorio suficientemente seguro.

b) El grado de clasificación se marcará claramente en el sobre interior o en la capa interior del envoltorio.

c) El exterior del envoltorio estará sellado y en este no se indicará la clasificación.

d) Los sobres o capas del envoltorio tanto interiores como exteriores estarán claramente dirigidos a una persona designada en la entidad destinataria prevista y llevarán un remite.

e) Dentro del sobre interior o la capa interior del sobre se incluirá un impreso de recibo de registro que el destinatario deberá cumplimentar y reenviar. El recibo de registro, que en sí mismo no estará clasificado, indicará el número de referencia, la fecha y el número de copias del documento, pero no deberá indicar el asunto.

f) En el sobre exterior o en la capa exterior del envoltorio se incluirá un recibo de entrega. El recibo de entrega, que en sí mismo no estará clasificado, indicará el número de referencia, la fecha y el número de copias del documento, pero no deberá indicar el asunto.

g) El servicio de mensajería deberá obtener y proporcionar al remitente una prueba de la entrega del envío en el registro de firma y recuento, u obtener recibos o los números de los paquetes.

3. Antes del envío, el remitente deberá ponerse en contacto con el destinatario designado para convenir una fecha y una hora de entrega apropiadas.

4. El remitente será el único responsable de los envíos expedidos mediante un servicio de mensajería comercial. En caso de que el envío se extravíe o no se entregue a tiempo, el remitente notificará la situación al responsable de seguridad de la información y al controlador del registro, quienes efectuarán un seguimiento del incidente de seguridad.

Artículo 26

Otras condiciones de manejo específicas

1. Se cumplirán todas las condiciones de transporte que se hayan establecido en un acuerdo sobre seguridad de la información o en un arreglo administrativo. En caso de duda, el personal consultará al responsable de seguridad de la información o al controlador del registro.

2. El requisito de doble envoltorio podrá ser inaplicado en el caso de la información clasificada que esté protegida por productos criptográficos aprobados. No obstante, a efectos de expedición, y debido al hecho de que los soportes de almacenamiento extraíble llevan una marca de clasificación de seguridad explícita, los soportes se transportarán al menos en un sobre sellado opaco y, si procede, se aplicarán otras medidas de protección física adicionales, como el uso de sobres recubiertos en el interior con plástico de burbujas.

CAPÍTULO 4

REUNIONES CLASIFICADAS

Artículo 27

Preparación de una reunión CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET

1. Las reuniones en las que esté previsto discutir información CONFIDENTIEL UE/EU CONFIDENTIEL o SECRET UE/EU SECRET se celebrarán solo en salas de reuniones que hayan sido acreditadas al nivel adecuado o superior. El Tribunal de Cuentas podrá usar salas de reunión en la zona de acceso restringido de otra institución de la UE. Cuando no estén disponibles, el personal buscará el asesoramiento del responsable de seguridad de la información.

2. Como regla general, los órdenes del día no deben clasificarse. El hecho de que el orden del día de alguna reunión haga referencia a documentos clasificados no implica que el orden del día deba clasificarse automáticamente. Los puntos del orden del día se formularán con una redacción que evite todo riesgo para los intereses de la Unión o de uno o más Estados miembros.

3. Los organizadores de las reuniones habrán de recordar a los participantes que las observaciones relativas a puntos CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET del orden del día no deben enviarse por correo electrónico, ni por otros medios que no hayan sido debidamente acreditados con arreglo al artículo 11 de la presente Decisión.

4. Los organizadores de las reuniones tratarán de agrupar de manera consecutiva en el orden del día los puntos CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET para facilitar el fluido desenvolvimiento de la reunión. Solo podrán estar presentes en el debate de los puntos clasificados las personas con necesidad de conocerlos, que dispongan de la habilitación de seguridad al nivel apropiado y que estén autorizadas.

5. En la propia invitación se prevendrá a los participantes de que en el orden del día se introducirán temas clasificados, lo que dará lugar a la aplicación de las medidas de seguridad adecuadas.

6. Los organizadores de las reuniones recordarán a los participantes que durante el debate de los puntos CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET deberán dejarse fuera de la sala de reunión los dispositivos electrónicos portátiles.

7. Antes de la reunión, los organizadores elaborarán una lista completa de los participantes. Conforme al artículo 4, apartado 6, de la Decisión n.º 41/2021, informarán a su debido tiempo al responsable de seguridad de la información de las fechas, horas y lugares de reunión y facilitará una relación de los participantes.

Artículo 28

Acceso de los participantes a una reunión CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU

1. Los organizadores de la reunión informarán al responsable de seguridad de la información y al controlador del registro de todo visitante externo que asista a una reunión CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET organizada por el Tribunal de Cuentas.

2. Para poder estar presentes en el debate de los puntos del orden del día CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, los participantes deberán demostrar que son titulares de una habilitación de seguridad válida del nivel apropiado.

Artículo 29

Equipo electrónico en las salas de reuniones CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET

Cuando se transmita información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, por ejemplo, durante una presentación o videoconferencia, solo podrán utilizarse sistemas informáticos acreditados con arreglo al artículo 11 de la presente Decisión.

Artículo 30

Procedimientos que han de seguirse durante las reuniones CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET

1. Al inicio del debate sobre temas clasificados, el presidente anunciará a los asistentes a la reunión que se pasa a «modo clasificado» Se cerrarán las puertas.

2. Solo se firmará para su recuento y se entregará a los participantes y a los intérpretes el número necesario de documentos, según corresponda, al inicio del debate.

3. Los documentos CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET no se dejarán desatendidos durante las pausas de la reunión.

4. Al término de la reunión, se recordará a los participantes y a los intérpretes que no dejen desatendidos en la sala los documentos clasificados o las notas clasificadas que hayan podido tomar. Todo documento CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET que no necesiten los participantes al término de la reunión y, en cualquier caso, los documentos de los intérpretes, se firmarán para su recuento y devolverán al controlador del registro para su destrucción en las trituradoras apropiadas ([9]).

5. Durante la reunión, se anotará la lista de participantes y se realizará una sinopsis de la información clasificada facilitada a los Estados miembros y comunicada verbalmente a terceros países u organizaciones internacionales para su registro en el resultado de los trabajos.

Artículo 31

Intérpretes y traductores

Solo los intérpretes y traductores con habilitación de seguridad y autorizados que estén sujetos al Estatuto de los funcionarios o al régimen aplicable a los otros agentes de la Unión Europea ([10]) o que tengan un vínculo contractual con el Tribunal de Cuentas u otra institución de la UE tendrán acceso a la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

([9]) Véase el artículo 42, apartado 6, para obtener más información.

([10]) Reglamento n.º 31 (CEE) por el que se establece el Estatuto de los funcionarios y el régimen aplicable a los otros agentes, modificado, (DO 45 de 14.6.1962, p. 1385/62) (ELI: hhttps://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:01962R0031-20230101).

CAPÍTULO 5

PUESTA EN COMÚN E INTERCAMBIO DE INFORMACIÓN CONFIDENTIEL UE/EU CONFIDENTIAL Y SECRET UE/EU SECRET

Artículo 32

Consentimiento del originador

Si el Tribunal de Cuentas no es la entidad originadora de la información clasificada que desea divulgar o poner en común, o del material original que esta pueda contener, el servicio del Tribunal de Cuentas que posea la información clasificada deberá recabar el consentimiento escrito del originador para divulgarla. Si no se puede identificar al originador, el Tribunal de Cuentas que posea esa información clasificada ejercerá el control de originador.

Artículo 33

Puesta en común de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET con otras entidades de la Unión

1. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET solo se pondrá en común con otra institución, agencia, organismo u oficina de la Unión si el destinatario tiene necesidad de conocerla y si dicha entidad tiene el correspondiente arreglo jurídico con el Tribunal de Cuentas.

2. Dentro del Tribunal de Cuentas, el Registro de ICUE será, por regla general, el punto principal de entrada y de salida para los intercambios de información clasificada con otras instituciones, órganos, organismos u oficinas de la UE.

Artículo 34

Intercambio de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET con los Estados miembros

1. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET podrá ponerse en común con los Estados miembros si el destinatario tiene necesidad de conocerla y dispone de una habilitación de seguridad.

2. La información clasificada de los Estados miembros que lleve una marca de clasificación nacional equivalente ([11]) y que haya sido facilitada al Tribunal de Cuentas recibirá el mismo grado de protección que la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET.

Artículo 35

Intercambio de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET con terceros países y organizaciones internacionales

1. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET solo se divulgará a un tercer país o a una organización internacional si el destinatario tiene necesidad de conocerla y el país u organización internacional dispone de un marco jurídico o administrativo apropiado, como un acuerdo de seguridad de la información o un arreglo administrativo con el Tribunal de Cuentas. Las disposiciones de dichos acuerdos o arreglos prevalecerán sobre las de la presente Decisión.

2. Por regla general, el Registro de la ICUE actuará como punto principal de entrada y de salida de toda la información clasificada CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET intercambiada entre el Tribunal de Cuentas y terceros países u organizaciones internacionales.

([11]) El cuadro de correspondencias de las marcas de los Estados miembros figura en el anexo I de la Decisión (UE, Euratom) 2015/444.

3. Toda información clasificada que se reciba de un tercer país o una organización internacional se registrará con fines de seguridad. Consiguientemente, el personal se pondrá en contacto con el Registro de la ICUE si recibe información clasificada que no proceda del circuito habitual del registro.

4. Para garantizar su rastreabilidad, la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se registrará:

— cuando llegue a la zona de acceso restringido o salga de ella, y

— cuando llegue a un SIC o salga de él.

5. Esta información podrá registrarse en papel o en libros de registro electrónicos.

6. Los procedimientos de registro de la información clasificada manejada en un SIC acreditado podrán llevarse a cabo mediante los procesos internos del propio SIC En ese caso, el SIC incluirá medidas para garantizar la integridad de los libros de registro.

7. La información clasificada recibida de terceros países o de organizaciones internacionales recibirá un grado de protección equivalente al de la ICUE que lleve la marca de clasificación equivalente, según se establezca en el acuerdo de seguridad de la información o en el arreglo administrativo correspondiente.

Artículo 36

Divulgación *ad hoc* con carácter excepcional de la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET

1. Cuando el Tribunal de Cuentas o alguno de sus servicios determine que existe una necesidad excepcional de divulgar información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET a un tercer país, una organización internacional o una entidad de la UE, pero no exista ningún acuerdo de seguridad de la información o arreglo administrativo, se aplicará el procedimiento de divulgación *ad hoc* con carácter excepcional.

2. Los servicios del Tribunal de Cuentas se pondrán en contacto con el responsable de seguridad de la información y el originador. El Tribunal de Cuentas consultará a una de las Partes de un acuerdo de seguridad de la información celebrado con esa misma entidad de la UE, tercer país u organización internacional.

3. Después de esta consulta, los Miembros del Tribunal de Cuentas, a propuesta del Secretario General, podrán autorizar la divulgación de dicha información.

CAPÍTULO 6

FIN DE VIDA ÚTIL DE LA INFORMACIÓN CONFIDENTIEL UE/EU CONFIDENTIAL Y SECRET UE/EU SECRET

Artículo 37

Rebaja de la clasificación y desclasificación

1. La información solo permanecerá clasificada mientras requiera protección. Por rebaja de la clasificación se entiende una reducción del grado de clasificación de seguridad. La desclasificación significará que la información dejará de considerarse clasificada desde todo punto de vista. Al producir la información, el originador indicará, siempre que sea posible, si puede rebajarse la clasificación de la ICUE o desclasificarse en una fecha determinada o tras un acontecimiento concreto. De no ser posible, el originador revisará la información y hará una evaluación de los riesgos, cada cinco años como mínimo, para determinar si el grado de clasificación original sigue siendo apropiado.

2. Los documentos del Tribunal de Cuentas también podrán ser objeto de una rebaja de clasificación o desclasificarse con carácter *ad hoc*, por ejemplo a raíz de una solicitud de acceso público.

Artículo 38

Responsabilidad de la rebaja de clasificación y la desclasificación

1. No se rebajará la clasificación de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET ni se desclasificará sin el permiso de su originador.

2. El servicio del Tribunal de Cuentas que cree un documento clasificado será responsable de decidir si puede desclasificarse o si puede rebajarse su clasificación. En el Tribunal de Cuentas, todas las solicitudes de rebaja de clasificación o de desclasificación serán sometidas a la consulta del gerente principal o director del servicio originario, o del jefe de tarea. Si el servicio ha compilado información clasificada procedente de diversas fuentes, deberá recabar, en primer lugar, el consentimiento de las otras partes que hayan facilitado material original, incluidos los Estados miembros, otros organismos de la UE, terceros países u organizaciones internacionales.

3. Cuando el servicio originario del Tribunal de Cuentas haya dejado de existir y sus responsabilidades hayan sido asumidas por otro servicio, será este último el que adopte la decisión sobre la rebaja de la clasificación o la desclasificación. Cuando el servicio originario haya dejado de existir y sus responsabilidades no hayan sido asumidas por otro servicio, la decisión sobre la rebaja de clasificación o la desclasificación será adoptada conjuntamente por los directores del Tribunal de Cuentas.

4. El servicio responsable de la rebaja de clasificación o la desclasificación colaborará con su Registro de la ICUE para adoptar las disposiciones prácticas necesarias con tal fin.

Artículo 39

Información sensible no clasificada

Cuando la revisión de un documento desemboque en una decisión de desclasificación, deberá considerarse si el documento debe llevar una marca de información sensible no clasificada conforme al apartado 16 de la política de clasificación de información del Tribunal de Cuentas ([12]) y al apartado 4 de las directrices sobre clasificación y manejo de información clasificada no perteneciente a la UE.

Artículo 40

Indicación de que se ha rebajado la clasificación de un documento o de que se ha desclasificado

1. La marca de clasificación original en la parte superior e inferior de cada página deberá tacharse de forma visible (no suprimirse) mediante la función «tachado», en el caso de los formatos electrónicos, o de forma manual, en los documentos impresos.

2. La primera página (cubierta) deberá llevar un sello que indique que el documento ha sido objeto de una rebaja del grado de clasificación o desclasificado y completarse con los datos de la autoridad responsable de la rebaja de clasificación o la desclasificación y la fecha correspondiente.

3. Se informará de la rebaja de clasificación o la desclasificación a los destinatarios originales de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET. Los destinatarios iniciales serán responsables de informar a los destinatarios subsiguientes a quienes hayan enviado la información original CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET o puesto en copia de su envío.

4. Se notificará al servicio de archivos del Tribunal de Cuentas de todas las decisiones de desclasificación que se adopten.

5. Todas las traducciones de información clasificada estarán sujetas a los mismos procedimientos de rebaja de clasificación o desclasificación que la versión lingüística original.

([12]) Puede consultarse en https://www.eca.europa.eu/es/legal-framework.

Artículo 41

Rebaja de clasificación parcial o desclasificación parcial de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. Será también posible una rebaja de clasificación parcial o una desclasificación parcial (que afecte, por ejemplo, a los anexos o a determinados apartados del documento). El procedimiento será idéntico al de rebaja de clasificación o desclasificación de un documento íntegro.

2. Tras la desclasificación parcial de la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, se producirá un extracto desclasificado.

3. En el extracto desclasificado, las partes que permanezcan clasificadas se sustituirán por la inscripción:

PARTE QUE NO DEBE DESCLASIFICARSE

bien en el cuerpo del texto, si la parte que permanece clasificada forma parte de un apartado, bien como apartado, si la parte que permanece clasificada ocupa uno o más apartados completos.

4. Cuando un anexo completo no pueda desclasificarse y, por lo tanto, no figure en el extracto, se hará una mención específica de esa circunstancia en el texto.

Artículo 42

Destrucción y eliminación rutinarias de información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET

1. El Tribunal de Cuentas no acumulará grandes volúmenes de información clasificada.

2. Al menos cada cinco años, los servicios originarios revisarán los documentos para su destrucción o eliminación. Se llevará a cabo una revisión a intervalos regulares tanto de la información almacenada en papel como de la almacenada en SIC.

3. El personal no destruirá ningún documento CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en soporte de papel que haya dejado de necesitar, sino que solicitará al controlador del registro que destruya esos documentos, sin perjuicio de los requisitos de archivo que se apliquen al documento original.

4. El personal no estará obligado a informar al originador de la eliminación de copias de documentos CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

5. Los borradores que contengan información clasificada serán sometidos a los mismos métodos de eliminación que los documentos clasificados finalizados.

6. Para la destrucción de los documentos CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET solo se utilizarán trituradoras aprobadas. Las trituradoras con el grado de seguridad 5 de la norma DIN 66399 se consideran adecuadas para la destrucción de documentos CONFIDENTIEL UE/EU CONFIDENTIAL. Las trituradoras con el grado de seguridad 6 de la norma DIN 66399 se consideran adecuadas para la destrucción de documentos SECRET UE/EU SECRET.

7. Los residuos de las trituradoras aprobadas podrán eliminarse como residuos de oficina normales.

8. El controlador del registro elaborará certificados de destrucción y actualizará consiguientemente los libros de registro electrónicos y demás información sobre el registro.

9. Todos los soportes y dispositivos que contengan información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET serán adecuadamente saneados cuando lleguen al final de su vida útil. Los datos electrónicos se destruirán o borrarán de los recursos informáticos y los soportes de almacenamiento asociados de una forma que ofrezca garantías suficientes de que la información no puede recuperarse. El saneamiento suprimirá los datos, así como todas las etiquetas, marcas y registros de actividad, del dispositivo de almacenamiento.

10. Los soportes de almacenamiento informático se entregarán al responsable de seguridad de la información para su destrucción y eliminación, después de que el controlador del registro haya sido informado.

Artículo 43

Evacuación y destrucción de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET en caso de emergencia

1. Conforme al memorando de entendimiento entre el Tribunal de Cuentas y la Dirección General de Recursos Humanos y Seguridad de la Comisión sobre la utilización de su zona de acceso restringido, se aplicará el procedimiento establecido de emergencia de la Comisión para la salvaguarda de la información clasificada. En caso necesario, el responsable de seguridad local de la dirección de seguridad de Luxemburgo de la Comisión tendrá acceso a la caja fuerte del Tribunal de Cuentas para aplicar el procedimiento de emergencia establecido de la Comisión y activar planes de evacuación de emergencia y de destrucción para salvaguardar la ICUE que se encuentre en riesgo alto de caer en manos no autorizadas durante una crisis. Por orden de prioridad y en función de la naturaleza de la emergencia, se barajarán las opciones siguientes:

i) trasladar la ICUE a otro lugar seguro, a ser posible una zona de acceso restringido dentro del mismo edificio;

ii) evacuar la ICUE a otro lugar seguro, a ser posible una zona de acceso restringido en otro edificio, preferentemente un edificio de una institución de la UE;

iii) destruir la ICUE, utilizando, en la medida de lo posible, los medios de destrucción aprobados.

2. Cuando se hayan activado planes de emergencia, se dará prioridad al traslado o la destrucción de la información SECRET UE/EU SECRET en primer lugar y, a continuación, de la información CONFIDENTIEL UE/EU CONFIDENTIAL.

3. A su vez, los detalles operativos de los planes de evacuación y destrucción de emergencia se clasificarán como RESTREINT UE/EU RESTRICTED. En cada caja fuerte en la que se guarde información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se conservará al menos una copia de forma que esté accesible en caso de emergencia.

Artículo 44

Archivo

1. Las decisiones sobre la necesidad de archivar, en qué momento, y las medidas prácticas correspondientes se adoptarán de conformidad con la política del Tribunal de Cuentas en materia de seguridad de la información, clasificación de información y archivo.

2. Los documentos CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET no se enviarán a los Archivos Históricos de la Unión Europea en Florencia.

CAPÍTULO 7

DISPOSICIONES FINALES

Artículo 45

Transparencia

La presente Decisión será puesta en conocimiento del personal del Tribunal de Cuentas y de las demás personas a las que se aplique, y se publicará en el *Diario Oficial de la Unión Europea*.

Artículo 46

Entrada en vigor

Tras su adopción por parte del Comité Administrativo, la presente Decisión entrará en vigor al día siguiente de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Luxemburgo, el 19 de marzo de 2024

Por el Comité Administrativo del Tribunal de Cuentas
El Presidente
Tony MURPHY

ANEXO

Categorías de personal que pueden tener acceso a información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET cuando así lo exija el desempeño de sus funciones

Categorías de personal del Tribunal de Cuentas	Acceso a la información CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET	Condiciones
Miembros	sí	Información + reconocimiento
Funcionarios	sí	Investigación + información + reconocimiento + autorización + necesidad de conocer
Agentes temporales	sí	Investigación + información + reconocimiento + autorización + necesidad de conocer
Agentes contractuales	sí	Investigación + información + reconocimiento + autorización + necesidad de conocer
Expertos nacionales en comisión de servicios de Estados miembros de la UE	sí	Solo si dispone de habilitación de seguridad de los Estados miembros originadores antes de asumir su cometido + información del Tribunal de Cuentas + reconocimiento + autorización del Tribunal de Cuentas + necesidad de conocer
Becarios	no	No cabe ninguna excepción
Cualquier otra categoría de personal (interinos, personal externo en régimen «intramuros», etc.)	no	No cabe ninguna excepción