REGLAMENTOS INTERNOS Y DE PROCEDIMIENTO

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)

EL TRIBUNAL DE CUENTAS EUROPEO,

Visto el artículo 13 del Tratado de la Unión Europea,

Visto el artículo 287 del Tratado de Funcionamiento de la Unión Europea,

Visto el artículo 257 del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión,

Visto el artículo 1, apartado 6, disposiciones de aplicación del Reglamento interno del Tribunal de Cuentas (Decisión n.º 21/2021 del Tribunal de Cuentas),

Vistas las normas de seguridad para la protección de la información clasificada de la UE de otras instituciones, órganos, o agencias de la Unión,

Vista la política de seguridad de la información del Tribunal de Cuentas (DEC 127/15 FINAL) y la política de clasificación de información (Circular 123/2020),

Considerando lo siguiente:

(1) De conformidad con el artículo 287, apartado 3, del TFUE, el Tribunal de Cuentas tiene derecho a acceder a cualquier documento o información que sean necesarios para llevar a cabo su labor, así como a información clasificada de la UE (ICUE), y que lo llevará a cabo cumpliendo plenamente con el principio de cooperación leal entre las instituciones y el principio de atribución; y que el derecho de acceso a la ICUE, garantizada por el TFUE, no podrá ser cuestionado por el originador de la ICUE; y considerando que se podrá pedir al Tribunal de Cuentas que establezca y cumpla ciertas medidas de seguridad que se detallan a continuación.

(2) Los Miembros del Tribunal de Cuentas Europeo, funcionarios y otros agentes están sujetos, incluso tras el cese de sus funciones, a una obligación de confidencialidad en virtud del artículo 339, del TFUE, del artículo 17 del Estatuto de los funcionarios o de los actos adoptados en virtud de los mismos.

(3) Por su carácter sensible, el tratamiento de la ICUE requiere que se garantice el cumplimiento de la obligación de confidencialidad mediante medidas apropiadas de seguridad que garanticen un alto nivel de protección de dicha información y que sean equivalentes a las establecidas por la normativa aplicable en otras instituciones, agencias y organismos de la UE en materia de protección de la ICUE, entendiéndose que, en caso de que el Tribunal de Cuentas, teniendo en cuenta la naturaleza y el tipo de ICUE, considere que dichas medidas de seguridad no están justificadas, se reservará el derecho a formular las observaciones que considere oportunas, respetando el nivel de clasificación de la ICUE.

(4) Las medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de información comunicada por el Tribunal de Cuentas serán adecuadas a la naturaleza y el tipo de la información de que se trate.

(5) Debe proporcionarse al Tribunal de Cuentas acceso a información clasificada en la medida en que sea necesario conocerla para ejecutar las tareas asignadas por los Tratados y por los actos jurídicos adoptados con arreglo a los Tratados.

(6) Por la naturaleza y el contenido sensible de algunas informaciones, procede establecer un procedimiento especial para el tratamiento por parte del Tribunal de Cuentas de documentos que contengan ICUE.

(7) La institución ha de garantizar que esta Decisión se aplique con arreglo a la normativa vigente, en particular las disposiciones relativas a la protección de datos personales, la seguridad física de las personas, los edificios y los sistemas informáticos.

DECIDE:

Artículo 1

Objeto y ámbito de aplicación

1. La presente Decisión establece los principios básicos y los estándares mínimos de seguridad para la protección de la información clasificada manejada por el Tribunal de Cuentas en el ejercicio de su mandato.

2. A efectos de la presente Decisión, por «información clasificada» se entenderá todos o algunos de los siguientes tipos de información:

a) «información clasificada de la UE (ICUE)» tal como se define en las normas de seguridad de otras instituciones, órganos y organismos de la UE etiquetada con alguna de las siguientes marcas de identificación:

   — TRES SECRET UE/EU TOP SECRET: Información y material cuya revelación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros,

   — SECRET UE/EU SECRET: Información y material cuya revelación no autorizada pueda causar un perjuicio grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros,

   — CONFIDENTIEL UE/EU CONFIDENTIAL: Información y material cuya revelación no autorizada pueda causar perjuicio a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros,

   — RESTREINT UE/EU RESTRICTED: Información y material cuya revelación no autorizada pueda resultar desfavorable para los intereses de la Unión Europea o de uno o varios Estados miembros;

b) información clasificada facilitada por los Estados miembros que lleve una marca nacional de clasificación de seguridad equivalente a las de la clasificación de seguridad ICUE ([1]) enumeradas en la letra a);

c) información clasificada facilitada al Tribunal de Cuentas Europeo por terceros Estados u organizaciones internacionales que lleve una marca nacional de clasificación de seguridad equivalente a las de la clasificación de seguridad ICUE enumeradas en la letra a) con arreglo a los acuerdos de seguridad de la información pertinentes.

3. El Tribunal de Cuentas tratará la información de grado RESTREINT UE/EU RESTRICTED en sus locales y aplicará las medidas de protección necesarias para ello. 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.

4. La presente Decisión se aplicará a todos los servicios del Tribunal de Cuentas y en todos sus locales.

5. Sin perjuicio de las indicaciones específicas relativas a grupos concretos de personal, la presente Decisión se aplicará a los Miembros del Tribunal de Cuentas, al personal del Tribunal de Cuentas incluido en el ámbito de aplicación del Estatuto de los funcionarios y de las condiciones de empleo de otros agentes de la Unión Europea ([2]), a los expertos nacionales enviados en comisión de servicio al Tribunal de Cuentas (en lo sucesivo, «expertos nacionales en comisión de servicios»), a los proveedores de servicios y su personal, a los trabajadores en prácticas y a cualquier persona con acceso a los edificios del Tribunal de Cuentas u otros activos, o a la información manejada por el Tribunal de Cuentas.

6. A menos que se especifique lo contrario, las disposiciones relativas a la ICUE se aplicarán de manera equivalente a la información clasificada prevista en el apartado 2, letras b) y c), del presente artículo.

([1]) Véase el Acuerdo entre los Estados miembros de la Unión Europea, reunidos en el seno del Consejo, sobre la protección de la información clasificada intercambiada en interés de la Unión Europea de (DO C 202 de 8.7.2011, p. 13) y su anexo.

([2]) 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) (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

Artículo 2

Definiciones

A efectos de la presente Decisión, se entenderá por:

a) «autorización para acceder a ICUE»: Decisión del Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas, adoptada sobre la base de una garantía concedida por una autoridad competente de un Estado miembro, que acredita que un funcionario u otro agente del Tribunal de Cuentas Europeo o experto nacional destinado en el Tribunal de Cuentas Europeo en comisión de servicio puede tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada. De la persona que se ajuste a esta descripción se dirá que tiene «autorización de seguridad»;

b) «clasificación»: Asignación de un nivel adecuado de clasificación a la información en función del grado de perjuicio que pudiera causar su divulgación no autorizada;

c) «material de cifra»: Algoritmos criptológicos, módulos criptológicos de *software* y *hardware*, y productos, incluida la información sobre su uso y la documentación pertinente y los datos de claves;

d) «desclasificación»: Supresión de toda clasificación de seguridad;

e) «documento»: Toda información registrada, independientemente de su soporte o características físicas;

f) «reducción del grado de clasificación»: Reducción del grado de clasificación de seguridad;

g) «habilitación de seguridad de establecimiento»: Certificación administrativa por parte de una ANS o ASD o cualquier otra autoridad de seguridad competente de que, desde el punto de vista de la seguridad, un determinado establecimiento puede brindar un nivel adecuado de protección a la ICUE de un grado específico de clasificación de seguridad;

h) «manejo» de ICUE: Toda intervención posible a la que puede estar sujeta a lo largo de su ciclo de vida la ICUE, es decir: producción, registro, tratamiento, traslado, reducción del grado de clasificación, desclasificación y destrucción. En relación con los sistemas de información y comunicaciones (SIC) abarca asimismo su recopilación, exposición, transmisión y almacenamiento;

i) «poseedor»: Persona debidamente autorizada con una probada necesidad de conocer la información, que está en posesión de cualquier ICUE y es, por tanto, responsable de su protección;

j) «autoridad de seguridad de la información»: Responsable de seguridad de la información del Tribunal de Cuentas, que podrá delegar, total o parcialmente, todas o parte de las competencias previstas en la presente Decisión;

k) «información»: Toda información escrita u oral, cualquiera que sea el soporte o el autor.

l) «material»: Todo medio, soporte de datos, máquina o aparato;

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

n) «habilitación personal de seguridad» (HPS): Declaración de una autoridad competente de un Estado miembro, efectuada al término de una investigación de seguridad realizada por las autoridades competentes del Estado miembro, mediante la cual se acredita que una persona puede, siempre que se haya determinado su «necesidad de conocer» y haya sido adecuadamente informada de sus responsabilidades, tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada;

o) «certificado de habilitación personal de seguridad» (CHPS): Certificado expedido por el Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas mediante el cual se establece que una persona dispone de un certificado de habilitación de seguridad o una autorización válidos para acceder a ICUE (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), el período de validez de la habilitación y la fecha de caducidad del propio certificado;

p) «autoridad de la seguridad física»: Jefe de Seguridad del Tribunal de Cuentas, responsable de la aplicación de las medidas y procedimientos de seguridad física necesarios para proteger la ICUE;

q) la «Oficina de Registro» será administrada por la Secretaría del Tribunal, ubicada en una Zona Administrativa bajo la responsabilidad del director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas. Será responsable de la entrada y salida de la información de grado RESTREINT UE/EU RESTRICTED o equivalente, intercambiada con el Tribunal de Cuentas;

r) el «registro de ICUE» se ubicará dentro de una Zona de Acceso Restringido. Dicho registro será gestionado por un controlador del registro del Tribunal de Cuentas que tenga una habilitación de seguridad. Será responsable de la entrada y salida de la información de grado CONFIDENTIEL UE/EU CONFIDENTIAL, superior o equivalente, intercambiada con el Tribunal de Cuentas;

s) «Autoridad de Acreditación de Seguridad (AAS)»: Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas.

Artículo 3

Medidas de seguridad para proteger la ICUE

1. El Tribunal de Cuentas garantizará la protección de toda la información clasificada que se le proporcione de manera acorde con el grado de clasificación de seguridad determinado por el originador y de conformidad con la presente Decisión.

2. Para ello, el Tribunal de Cuentas someterá el manejo de ICUE a medidas de seguridad físicas y de personal como autorizaciones de acceso para las personas identificadas y medidas de protección de los sistemas de comunicación e información. Estas medidas se describen en los artículos 4 a 6 y serán aplicables a lo largo de todo el ciclo de vida de la ICUE. Serán acordes con su clasificación de seguridad, la forma y el volumen de la información o material, la ubicación y construcción de la instalación en la que se conserve, y la amenaza de actividades maliciosas o delictivas, evaluadas localmente, en particular el espionaje, el sabotaje y el terrorismo.

3. La ICUE estará protegida por medidas de seguridad físicas, y la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se protegerá además con medidas de seguridad de personal.

4. La ICUE solo se facilitará a personas que tengan necesidad de conocer dentro de la institución. La persona que esté en posesión de cualquier ICUE será responsable de su protección de conformidad con la presente Decisión.

5. La ICUE no será revelada oralmente ni por escrito. Las observaciones preliminares, informes, dictámenes, comunicados de prensa y otros productos del Tribunal de Cuentas, su sitio web y su intranet, intervenciones orales, respuestas a solicitud de acceso a documentos ([3]) y grabaciones de voz o de vídeo no deberán contener ICUE o extractos de la misma ni hacer referencia a ella. No obstante, si el originador ha publicado documentos o información que contengan referencias a ICUE, podrá mencionarse dicha referencia.

6. No obstante lo dispuesto en el apartado 5, el Tribunal de Cuentas y el originador podrán acordar, en el caso de una auditoría específica, que el Tribunal de Cuentas pueda reproducir o utilizar elementos de ICUE en un documento. En tal caso, dicho documento del Tribunal de Cuentas se remitirá en primer lugar al originador de la ICUE de que se trate antes del procedimiento contradictorio o durante el mismo. Si se produce esta situación, el Tribunal de Cuentas y el originador acordarán si se clasificará el documento emitido por el Tribunal de Cuentas. Si un Miembro ponente del Tribunal de Cuentas considera necesario comunicar un informe de auditoría que haya sido clasificado total o parcialmente a determinados destinatarios del Parlamento Europeo o del Consejo, habida cuenta de todas las medidas de seguridad previstas en la presente Decisión, necesitará el consentimiento del originador de la información clasificada. El marco jurídico y el procedimiento para el intercambio de dichos documentos se establece en el artículo 7.

7. Cuando, en el ejercicio de su mandato, el Tribunal de Cuentas necesite compartir con más destinatarios determinados elementos de un documento clasificado, deberá consultarlo con el originador, teniendo debidamente en cuenta la marca de clasificación de seguridad, antes de decidir el uso de dichos elementos o información, si considera que hacerlo reviste un interés público superior. La información solo se utilizará en el informe de manera que no se perjudique el interés del originador. Dicho interés podrá salvaguardarse de manera apropiada pidiendo al originador que formule comentarios para llegar a un acuerdo sobre el modo de anonimizar, condensar o generalizar la información, etc., respetando a la vez los intereses de los principales afectados por la información publicada.

([3]) Con arreglo a la Decisión n.º 12/2005 del Tribunal de Cuentas Europeo relativa al acceso público a los documentos del Tribunal, modificada por la Decisión n.º 14/2009 (DO C 67 de 20.3.2009, p. 1).

8. El Tribunal de Cuentas no facilitará ICUE a otra institución, órgano, oficina o agencia de la UE, Estado miembro, tercer Estado u organización internacional sin consultar previamente al originador y sin el consentimiento expreso por escrito del mismo.

9. A menos que el originador de un documento clasificado de grado SECRET UE/EU SECRET o inferior haya impuesto restricciones a la duplicación o traducción del mismo, estos documentos podrán ser duplicados o traducidos a petición del poseedor y en cumplimiento de las instrucciones de trabajo prácticas de la autoridad de seguridad de la información en el Tribunal de Cuentas. Las medidas de seguridad aplicables al documento original también se aplicarán a las copias y traducciones de los mismos.

10. Si el Tribunal de Cuentas necesita un documento clasificado que ha recibido, o cuenta con autorización para acceder a él, para poder rebajar el grado de clasificación o desclasificarlo deberá consultar con el originador para preguntarle si puede proporcionarle una versión con el grado de clasificación rebajado o desclasificada.

Artículo 4

Seguridad en el personal

1. En virtud de sus funciones, los Miembros del Tribunal de Cuentas están autorizados para acceder a toda la ICUE o para asistir a reuniones en las que se maneje ICUE. Los Miembros serán informados de sus obligaciones de seguridad en materia de protección de la ICUE y reconocerán por escrito su responsabilidad de protección de dicha información.

2. Solo se concederá acceso a ICUE a miembros del personal del Tribunal de Cuentas Europeo, ya sean funcionarios, personal sujeto al Estatuto de los funcionarios de la Unión Europea y al régimen aplicable a los otros agentes de la Unión Europea o expertos nacionales en comisión de servicios:

i) cuya necesidad de conocer se haya determinado,

ii) que hayan sido instruidos sobre las normas de seguridad para la protección de la ICUE y las correspondientes directrices y estándares de seguridad, y que hayan aceptado sus responsabilidades en lo que respecta a la protección de dicha información,

iii) en el caso de información de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior: a quien se haya concedido una habilitación en el grado correspondiente, o bien a quien se haya autorizado debidamente.

3. El procedimiento para determinar si un funcionario u otro agente del personal del Tribunal de Cuentas está autorizado a acceder a información de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, teniendo en cuenta la lealtad, integridad y fiabilidad de la persona, una vez obtenidas las garantías de las autoridades competentes de un Estado miembro según lo previsto en el artículo 2, letra n) se establecerá en una decisión delegada, adoptada de conformidad con el artículo 10, apartado 10. Las decisiones para conceder autorización de acceso serán adoptadas por el Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas.

4. El Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas puede emitir certificados de habilitación personal de seguridad (CHPS) especificando el grado de clasificación para el que puede concederse a las personas acceso a ICUE (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), el período de validez de la correspondiente autorización de acceso y la fecha de vencimiento del CHPS.

5. Solo las personas con la autorización mencionada en el apartado 2, inciso iii), y los Miembros del Tribunal de Cuentas pueden, con arreglo al apartado 1, participar en reuniones en las que se maneje información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. El Tribunal de Cuentas y el originador adoptarán las medidas prácticas necesarias para estas reuniones caso por caso.

6. Los servicios del Tribunal de Cuentas responsables de la organización de reuniones en las que se maneje información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior informará a su debido tiempo a la autoridad de seguridad de la información de las fechas, horas y lugares de reunión y facilitará una relación de los participantes.

7. .Toda persona en posesión de ICUE sin la debida autorización ni probada necesidad de conocer debe notificar la situación a la autoridad de seguridad de la información lo antes posible y asegurarse de que la ICUE está protegida con arreglo a lo dispuesto en la presente Decisión.

Artículo 5

Medidas de seguridad física para la protección de la información clasificada

1. Se entenderá por «seguridad física» la aplicación de medidas de protección física y técnica para impedir el acceso no autorizado a ICUE.

2. Las medidas de seguridad física estarán concebidas para impedir la entrada, subrepticia o por la fuerza, de intrusos, para disuadir, impedir y descubrir actividades no autorizadas y para segregar al personal en lo que respecta al acceso a ICUE según el principio de necesidad de conocer el contenido de dicha información. Estas medidas se determinarán a partir de un proceso de gestión de riesgos, de conformidad con la presente Decisión.

3. Las zonas en que se maneje o se almacene ICUE serán inspeccionadas periódicamente por la autoridad de seguridad del Tribunal de Cuentas.

4. Para la protección de ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior solo podrán emplearse equipos o dispositivos que cumplan la normativa aplicable en las instituciones, agencias u organismos de la UE.

5. El personal del Tribunal de Cuentas tendrá acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, o el equivalente en zonas de acceso restringido fuera de los locales del Tribunal de Cuentas.

6. El Tribunal de Cuentas podrá suscribir un Acuerdo de Nivel de Servicio con otra institución de la UE en Luxemburgo para poder manejar y almacenar información de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior en una zona de acceso restringido de dicha institución. A menos que el originador lo acepte específicamente, dicha ICUE no se manejará ni almacenará en los locales del Tribunal de Cuentas, que tampoco podrá duplicarla ni traducirla.

7. La información RESTREINT UE/EU RESTRICTED recibida será registrada por el Tribunal de Cuentas. La consulta de información de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, o su equivalente, que tenga lugar fuera de los locales del Tribunal de Cuentas, será registrada a efectos de seguridad.

8. La ICUE de grado RESTREINT UE/EU RESTRICTED se podrá guardar en muebles de oficina adecuadamente cerrados con llave en las zonas administrativas o las zonas de acceso restringido. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se almacenará en virtud de un Acuerdo de Nivel de Servicio en una zona de acceso restringido dentro de un contenedor de seguridad de otra institución de la UE en Luxemburgo.

9. Cuando no esté inscrita en el registro, la ICUE se trasladará entre servicios y locales del siguiente modo:

a) como norma general, la ICUE se transmitirá por medios electrónicos que estén protegidos con productos criptológicos aprobados de conformidad con lo dispuesto en el artículo 6, apartado 8;

b) en caso de no utilizarse los medios contemplados en la letra a), la ICUE se transportará utilizando un soporte de datos (por ejemplo, llaves USB, discos compactos o discos duros) que estén protegidos con productos criptológicos aprobados de conformidad con lo dispuesto en el artículo 6, apartado 8, o en soporte de papel en un sobre cerrado opaco.

10. La información de grado RESTREINT UE/EU RESTRICED podrá ser destruida por su poseedor con arreglo a las normas de archivado aplicables en el Tribunal de Cuentas. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior será destruida por el controlador del registro por orden de su poseedor o de una autoridad competente con arreglo a las normas de archivado aplicables en el Tribunal de Cuentas. Los documentos clasificados de grado SECRET UE/EU SECRET serán destruidos en presencia de un testigo, que deberá estar habilitado como mínimo para el grado de clasificación del documento que se vaya a destruir. El controlador del registro, y el testigo en caso de que se requiera su presencia, firmarán un certificado de destrucción, que se archivará en el registro. El controlador del registro conservará los certificados de destrucción de los documentos de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET durante cinco años como mínimo.

11. La autoridad de seguridad física y la autoridad de seguridad de la información prepararán un plan conjunto, basados en las condiciones locales para proteger la ICUE en situaciones de crisis, incluidos, si fuera necesario, planes de destrucción y evacuación de urgencia. Promulgarán las instrucciones que se estimen necesarias para impedir que la ICUE caiga en manos de personas no autorizadas.

12. Cuando sea necesario transportar ICUE físicamente, el Tribunal de Cuentas cumplirá las medidas impuestas por el originador para protegerla de la divulgación no autorizada durante el transporte.

13. Las medidas de seguridad física que se aplicarán en las zonas administrativas en las que se maneja y almacena información de grado RESTREINT UE/EU RESTRICTED se enumeran en el anexo.

Artículo 6

Protección de la ICUE en los sistemas de información y comunicaciones

1. A efectos del presente artículo, se entiende por «sistema de información y comunicaciones» un sistema que permite manejar la ICUE en formato electrónico. Un sistema de información y comunicaciones abarca todos los medios necesarios para su funcionamiento, incluidos la infraestructura, la organización y los recursos de personal e información.

2. Por «legítimo usuario» se entiende un Miembro, funcionario u otro agente del Tribunal de Cuentas o experto nacional destinado al Tribunal de Cuentas que tenga una necesidad establecida y reconocida de acceder a un sistema específico de información.

3. El Tribunal de Cuentas ofrecerá garantías de que sus sistemas protegerán la información que manejan en un grado adecuado y que funcionarán como es necesario que lo hagan, cuando así se precise, bajo el control de sus legítimos usuarios. Para ello, garantizarán niveles adecuados de:

— autenticidad: La garantía de que la información es verídica y procede de fuentes de buena fe,

— disponibilidad: La propiedad de ser accesible y utilizable en el momento que lo requiera una entidad autorizada,

— confidencialidad: La propiedad de que la información no se divulgue a personas, organismos o procesos no autorizados,

— integridad: La propiedad de salvaguardar la exactitud y completitud de la información y los activos,

— no repudio: La capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente.

Esta garantía se basará en un proceso de gestión de riesgos. «Riesgo»: Posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades internas o externas de una organización o de cualquier sistema que esta utilice y al hacerlo ocasione daños a la organización o a sus activos tangibles o intangibles. Se mide como la combinación de la probabilidad de que se cumplan las amenazas y de su repercusión. El proceso de gestión de riesgos constará de las siguientes etapas: identificación de amenazas y vulnerabilidades, evaluación del riesgo, gestión del riesgo, aceptación del riesgo y comunicación del riesgo.

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

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

— «Aceptación del riesgo»: Decisión de aceptar, una vez tratado el riesgo, la persistencia de un riesgo residual.

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

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

4. Todos los dispositivos y equipos electrónicos utilizados para manejar ICUE deberán cumplir las normas aplicables para la protección de la ICUE. Se concederá preferencia a los dispositivos y equipos electrónicos que ya hayan sido autorizados por otra institución, órgano, oficina o agencia de la UE. La seguridad de los dispositivos deberá estar garantizada para todo su ciclo de vida.

5. El sistema de comunicación e información del Tribunal de Cuentas para manejar la ICUE deberá estar acreditada por una autoridad apropiada. Para ello, el Tribunal de Cuentas tratará de alcanzar un Acuerdo de Nivel de Servicio con una Autoridad de Acreditación de Seguridad de una institución de la UE que esté habilitada para autorizar el manejo de ICUE por un sistema de información y comunicaciones, con objeto de obtener una declaración de acreditación para información de grado RESTREINT UE/EU RESTRICTED que pueda ser manejada en el sistema de información y comunicaciones del Tribunal de Cuentas, así como las condiciones correspondientes para la operación. El Acuerdo de Nivel de Servicio también se referirá a las normas aplicables en el proceso de acreditación y se suscribirá con arreglo al procedimiento establecido en el artículo 10, apartado 3.

6. En caso de que el Tribunal de Cuentas tenga que establecer su propio proceso de acreditación para su Acuerdo de Nivel de Servicio, el proceso se establecerá en una decisión delegada según lo previsto en el artículo 10, apartado 10, de la presente Decisión con arreglo a las normas relativas al proceso de acreditación para el manejo de ICUE por un sistema de información y comunicaciones en otras instituciones, órganos y organismos de la UE.

7. La responsabilidad de la preparación de los expedientes de acreditación y la documentación con arreglo a la normativa aplicable será plenamente del propietario del sistema de información y comunicaciones.

8. Cuando la ICUE está protegida con productos criptológicos, el Tribunal de Cuentas concederá preferencia a los productos aprobados por el Consejo o por el Secretario General del Consejo en su calidad de autoridad de certificación criptológica, o a los aprobados por otras instituciones, órganos y organismos de la UE para la protección de ICUE.

9. La información RESTREINT UE/EU RESTRICTED solo se manejará en dispositivos electrónicos (como estaciones de trabajo, impresoras y fotocopiadoras) situados en zonas administrativas o en zonas de acceso restringido. Los dispositivos electrónicos en los que se maneje información de grado RESTREINT UE/EU RESTRICTED se segregarán de otras redes informáticas y se protegerán mediante medidas físicas o técnicas apropiadas.

10. Todo el personal involucrado en el diseño, desarrollo, prueba, operación, gestión o utilización de los sistemas de información y comunicaciones que manejen ICUE notificará al responsable de seguridad de la información todos los posibles puntos débiles, incidentes, fallos de seguridad o comprometimientos que puedan tener un impacto en la protección de los sistemas de información y comunicaciones o de la ICUE que contengan.

Artículo 7

Procedimiento para el intercambio de información clasificada y para permitir el acceso a la misma

1. Cuando están legalmente obligados a hacerlo en virtud de los Tratados o actos jurídicos adoptados con arreglo a los Tratados, las instituciones, órganos, organismos y agencias de la UE, y las autoridades nacionales, por propia iniciativa o previa petición por escrito del Presidente, del Miembro ponente o del Secretario General, proporcionarán acceso a ICUE al Tribunal de Cuentas siguiendo el procedimiento que se detalla a continuación.

2. Las solicitudes de acceso se remitirán a las instituciones interesadas a través de la Oficina de Registro del Tribunal de Cuentas.

3. En caso necesario, el Tribunal de Cuentas suscribirá un acuerdo administrativo que cubra los aspectos prácticos del intercambio de ICUE o equivalente.

4. A fin de concluir dichos acuerdos administrativos, el Tribunal de Cuentas facilitará al originador toda la información necesaria sobre su sistema de seguridad de la información. En caso necesario, puede organizarse una visita de evaluación.

5. Estos acuerdos administrativos se celebrarán cumpliendo plenamente los principios de cooperación leal y de atribución establecidos en el artículo 13 del Tratado de la Unión Europea. Se celebrarán de conformidad con el procedimiento establecido en el artículo 10, apartado 4.

6. Cuando no existan acuerdos administrativos con una institución, órgano u organismo de la UE, tercer Estado u organización internacional sobre el suministro de información clasificada al Tribunal de Cuentas, el Tribunal de Cuentas firmará una declaración de compromiso para proteger la información clasificada que reciba.

Artículo 8

Fallos de seguridad, pérdida o comprometimiento de información clasificada

1. Un. fallo de seguridad se produce como resultado de una acción u omisión de una persona contraria a las normas de seguridad establecidas en la presente Decisión y sus normas de desarrollo.

2. Se produce un comprometimiento de la ICUE cuando, como consecuencia de un fallo de seguridad, dicha información se pone total o parcialmente en conocimiento de personas no autorizadas.

3. Todo fallo o posible fallo de seguridad deberá comunicarse inmediatamente a la autoridad de seguridad del Tribunal de Cuentas.

4. Cuando se tenga conocimiento o sospechas fundadas de que una ICUE se ha visto comprometida o se ha perdido, la autoridad de seguridad de la información lo comunicará al Director de Recursos humanos, finanzas y servicios generales y al Secretario General del Tribunal de Cuentas. El Director de Recursos humanos, finanzas y servicios generales informará inmediatamente a la autoridad de seguridad correspondiente del originador. Dicho Director del Tribunal de Cuentas realizará una investigación de seguridad, e informará al Secretario General del Tribunal de Cuentas y la autoridad de seguridad del originador de sus resultados y de las medidas adoptadas para evitar que se reproduzca la misma situación. Cuando la situación afecte a un Miembro del Tribunal de Cuentas, el Presidente del Tribunal de Cuentas se encargará de tomar las medidas necesarias en colaboración con el Secretario General del Tribunal de Cuentas.

5. Cualquier funcionario u otro agente del personal del Tribunal de Cuentas que sea responsable de un fallo de las normas de seguridad establecidas en la presente Decisión y sus normas de desarrollo podrá ser objeto de medidas disciplinarias de conformidad con el Estatuto de los funcionarios y de las condiciones de empleo de otros agentes de la Unión Europea.

6. Cualquier Miembro del Tribunal de Cuentas que no cumpla las condiciones de esta Decisión podrá ser objeto de medidas y sanciones previstas en el artículo 286, apartado 6, del Tratado.

7. La persona que sea responsable de un comprometimiento o pérdida de ICUE podrá ser objeto de medidas disciplinarias o de una acción judicial de conformidad con las disposiciones legales y reglamentarias aplicables.

Artículo 9

Seguridad en caso de intervención exterior

1. El Tribunal de Cuentas podrá encomendar a contratistas registrados en un Estado miembro el cumplimiento de tareas que, en virtud de su contrato, impliquen o requieran el acceso a ICUE. Esto puede ocurrir concretamente con respecto al mantenimiento de los sistemas informáticos y de comunicaciones y de la red informática.

2. En caso de intervención exterior, el Tribunal de Cuentas aplicará todas las medidas necesarias previstas en el apartado 3 del presente artículo y solicitará una habilitación de seguridad de establecimiento para garantizar la protección de la ICUE por parte de candidatos y contratistas todo el período de vigencia del proceso de licitación y adjudicación de contratos públicos y por los contratistas y subcontratistas durante todo el período de vigencia del contrato. El poder adjudicador garantizará que en los contratos se recogen las normas mínimas de seguridad pr.evistas en las presente Decisión para obligar a los contratistas a cumplirlas.

3. Las normas de seguridad, los procedimiento de adjudicación de contratos, las plantillas y modelos de contratos y subcontratos que impliquen acceso a ICUE, anuncios de contrato, orientación sobre las circunstancias en que se requiere una habilitación de seguridad de establecimiento y de plantilla, instrucciones de seguridad de un programa o proyecto, cláusulas sobre aspectos de la seguridad, visitas, y transmisión y transporte de ICUE en virtud de contratos o acuerdos de subvención clasificados deberán ajustarse a las normas, plantillas y modelos establecidos por la Comisión Europea para contratos clasificados en la Decisión (UE, Euratom) 2015/444 de la Comisión ([4]).

([4]) 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).

Artículo 10

Aplicación de la presente Decisión y responsabilidades asociadas

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

2. El Secretario General será la autoridad facultada para proceder a los nombramientos y la autoridad facultada para celebrar los contratos de personal para funcionarios y otros agentes. El Secretario General podrá delegar en el Director de Recursos humanos, finanzas y servicios generales la responsabilidad de otorgar a los funcionarios y otros agentes autorización para acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, para ejercer su función de Autoridad de Acreditación de Seguridad y para supervisar la Secretaría del Tribunal en el manejo de ICUE.

3. El Secretario General será competente para suscribir acuerdos de nivel de servicio sobre la acreditación de equipos y sistemas de información y comunicaciones, sobre el uso de una zona de acceso restringido en otra institución de la UE y el procedimiento de solicitud de Certificado de habilitación personal de seguridad para acceder a ICUE.

4. El Director de Recursos humanos, finanzas y servicios generales será competente para celebrar acuerdos administrativos con las instituciones, agencias y otros organismos de la UE para el intercambio de ICUE, que el Tribunal de Cuentas exige para cumplir su mandato. Dicho director también podrá concluir acuerdos administrativos con terceros Estados u organizaciones internacionales para proteger toda la información clasificada recibida.

5. El Director de Recursos humanos, finanzas y servicios generales estará facultado para firmar cualquier declaración de compromiso de proteger la ICUE que se facilite en el contexto de una divulgación excepcional *ad hoc*.

6. El responsable de la seguridad de la información del Tribunal de Cuentas actuará como autoridad de seguridad de la información. El responsable de la seguridad de la información y las personas en las que delegue total o parcialmente sus funciones contarán con una habilitación de seguridad adecuada. La autoridad de seguridad de la información asumirá sus funciones en estrecha colaboración con la dirección de Recursos humanos, finanzas y servicios generales, la dirección de Información, entorno de trabajo e innovación y la dirección del Comité de control de calidad de la auditoría (véanse en particular los artículos 4, 6 y 8). La autoridad de seguridad de la información también será responsable de formación y reuniones de concienciación sobre la seguridad de la información, así como de inspecciones periódicas para comprobar el cumplimiento de la presente Decisión, también en caso de intervención exterior y de la aplicación de medidas para garantizar el cumplimiento.

7. El Jefe de Seguridad será responsable de las medidas de seguridad física (en particular el artículo 5).

8. La Oficina de Registro establecida en la Secretaría del Tribunal será el punto de entrada y salida de la información clasificada de grado RESTREINT UE/EU RESTRICTED que el Tribunal de Cuentas pueda intercambiar con las instituciones, agencias y otros organismos de la UE. También será el punto de entrada y salida de información equivalente de terceros Estados y organizaciones internacionales. La Oficina de Registro se organizará según los establecido en una decisión delegada. El responsable de la Oficina de Registro asumirá las siguientes responsabilidades principales:

a) registro de la entrada y salida de la información de grado RESTREINT UE/EU RESTRICTED;

b) gestión de zonas administrativas específicas para registrar el manejo, almacenamiento y consulta de ICUE clasificada de grado RESTREINT UE/EU RESTRICTED.

9. Deberá establecerse un Registro con arreglo a un Acuerdo de Nivel de Servicio sobre el uso de la zona de acceso restringido de otra institución de la UE. Este Registro organizado por la Secretaría del Tribunal bajo la responsabilidad del Director de Recursos humanos, finanzas y servicios generales del Tribunal de Cuentas será el punto de entrada y salida de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior que el Tribunal de Cuentas pueda intercambiar con otras instituciones, órganos y organismos de la UE y los Estados miembros. También será el punto de

entrada y salida para información equivalente de terceros Estados y organizaciones internacionales. Estará equipada con cajas fuertes apropiadas y otros equipos de seguridad apropiados para proteger información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior. El Registro se organizará según los establecido en una decisión delegada. El controlador del registro contará con una habilitación de seguridad adecuada y asumirá las siguientes responsabilidades principales:

a) gestión de operaciones relacionadas con el registro, la consulta, la preservación, la reproducción, la traducción, la transmisión, el envío, y, en su caso, la destrucción de ICUE;

b) desempeñar otras tareas relacionadas con la protección de ICUE definidas en una decisión delegada.

10. El Comité Administrativo adoptará una decisión delegada por la que se establecen normas de aplicación de la presente Decisión. El responsable de seguridad de la información establecerá directrices de seguridad de la información. El Comité de control de calidad de la auditoría elaborará directrices de auditoría.

Artículo 11

Entrada en vigor

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

Hecho en Luxemburgo, el 3 de junio de 2021.

Por el Tribunal de Cuentas
Klaus-Heiner LEHNE
Presidente

ANEXO

MEDIDAS DE SEGURIDAD FÍSICAS DE LAS ZONAS ADMINISTRATIVAS PARA ICUE

1. El presente anexo contiene normas de aplicación del artículo 5 de la Decisión. Estas son las normas mínimas relativas a la protección física de las zonas administrativas para información de grado RESTREINT UE/EU RESTRICTED en el Tribunal de Cuentas: zonas concebidas para el registro, almacenamiento y consulta de información clasificada de grado RESTREINT UE/EU RESTRICTED.

2. El propósito de las medidas de seguridad física en las zonas administrativas es impedir el acceso no autorizado a estas zonas del siguiente modo:

   a) se establecerá un perímetro visiblemente definido que permita el control de las personas;

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

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

3. Excepcionalmente, la autoridad de seguridad de la información del Tribunal de Cuentas podrá conceder acceso a personas sin autorización, también para trabajar en la zona administrativa, siempre que ello no implique acceso a ICUE, que permanecerá cerrado. Estas personas solo podrán entrar si están acompañadas y constantemente vigiladas por la autoridad de seguridad de la información o el controlador del registro.

4. La autoridad de seguridad de la información establecerá procedimientos de gestión de las llaves y las combinaciones utilizadas para todas las zonas administrativas y el mobiliario de seguridad. El propósito de estos procedimientos será garantizar la protección frente a accesos no autorizados.

5. Las combinaciones deberán ser memorizadas por el menor número posible de personas que necesiten conocerlas. Las combinaciones del mobiliario de seguridad empleado para el almacenamiento de información de grado RESTREINT UE/EU RESTRICTED se modificarán:

   — al recibir un nuevo mueble de seguridad;

   — cada vez que se produzca un cambio en el personal que conoce la combinación;

   — si se ha descubierto, o se sospecha que se ha descubierto, una combinación secreta;

   — si la cerradura se ha sometido a mantenimiento o reparación;

   — como mínimo cada 12 meses;

6. La autoridad de seguridad de la información y el Jefe de Seguridad serán responsables del cumplimiento de estas normas.