DECISIÓN (UE, Euratom) 2019/1963 DE LA COMISIÓN

de 17 de octubre de 2019

por la que se establecen normas de desarrollo sobre la seguridad industrial en relación con los contratos públicos clasificados

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 249,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica, y en particular su artículo 106,

Vista la Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión ([1]),

Vista 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 ([2]),

Vista la Decisión (UE, Euratom) 2017/46 de la Comisión, de 10 de enero de 2017, sobre la seguridad de los sistemas de información y comunicación de la Comisión Europea ([3]),

Previa consulta al grupo de expertos de seguridad de la Comisión, de conformidad con el artículo 41, apartado 5, de la Decisión (UE, Euratom) 2015/444,

Considerando lo siguiente:

(1) Los artículos 41, 42, 47 y 48 de la Decisión (UE, Euratom) 2015/444 establecen que las normas de desarrollo sobre seguridad industrial que se adopten deberán contener disposiciones más pormenorizadas para completar y facilitar la aplicación del capítulo 6 de dicha Decisión; dichas disposiciones deberán regular cuestiones como la licitación, la celebración de contratos clasificados, las habilitaciones de seguridad de establecimiento, las habilitaciones personales de seguridad, las visitas, y la transmisión y el transporte de información clasificada de la Unión Europea («ICUE»).

(2) La Decisión (UE, Euratom) 2015/444 establece que los contratos clasificados deben ejecutarse con la colaboración de la autoridad nacional de seguridad, la autoridad de seguridad designada o cualquier otra autoridad competente de los Estados miembros afectados; los Estados miembros han acordado garantizar que cualquier entidad bajo su jurisdicción que pueda recibir o generar información clasificada procedente de la Comisión esté debidamente habilitada y sea capaz de proporcionar una protección adecuada equivalente a la concedida por las normas de seguridad del Consejo de la Unión Europea para la protección de la ICUE con la marca de clasificación correspondiente, según se establece en 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 ([4]).

(3) El Consejo, la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad han acordado garantizar la máxima coherencia en la aplicación de las normas de seguridad en lo que respecta a su protección de la ICUE, teniendo en cuenta al mismo tiempo sus necesidades institucionales y organizativas específicas, de conformidad con las declaraciones adjuntas al acta de la sesión del Consejo en la que se adoptó la Decisión 2013/488/UE del Consejo ([5]), sobre las normas de seguridad para la protección de la información clasificada de la UE.

(4) Por consiguiente, las normas de desarrollo sobre la seguridad industrial en relación con los contratos clasificados de la Comisión también deben garantizar la máxima coherencia y tener en cuenta las Directrices sobre seguridad industrial aprobadas por el Comité de Seguridad del Consejo el 13 de diciembre de 2016 y los artículos 7 y 22 de la Directiva 2009/81/CE del Parlamento Europeo y del Consejo ([6]).

(5) El 4 de mayo de 2016, la Comisión adoptó una Decisión ([7]) por la que habilitaba al miembro de la Comisión responsable de los asuntos de seguridad a adoptar, en nombre de la Comisión y bajo la responsabilidad de esta, las normas de desarrollo contempladas en el artículo 60 de la Decisión (UE, Euratom) 2015/444.

([1]) DO L 72 de 17.3.2015, p. 41.
([2]) DO L 72 de 17.3.2015, p. 53.
([3]) DO L 6 de 11.1.2017, p. 40.
([4]) DO C 202 de 8.7.2011, p. 13.
([5]) Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).
([6]) Directiva 2009/81/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad (DO L 216 de 20.8.2009, p. 76).
([7]) Decisión de la Comisión, de 4.5.2016, relativa a una habilitación en materia de seguridad [C(2016) 2797 final].

HA ADOPTADO LA PRESENTE DECISIÓN:

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Decisión establece normas de desarrollo sobre la seguridad industrial en relación con los contratos públicos clasificados para contribuir a la ejecución de la Decisión (UE, Euratom) 2015/444 y, en particular, el capítulo 6 de dicha Decisión.

2. La presente Decisión establece requisitos específicos para garantizar la protección de la información clasificada de la UE («ICUE») por parte de los operadores económicos en la fase precontractual, a lo largo de todo el ciclo de vida de los contratos clasificados celebrados por la Comisión Europea, y en los subcontratos celebrados por los contratistas de la Comisión.

3. La presente Decisión se refiere a información clasificada de los grados siguientes:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Artículo 2

Responsabilidad dentro de la Comisión

1. Como parte de las responsabilidades descritas en el Reglamento Financiero ([8]), cada ordenador del órgano de contratación de la Comisión se asegurará de que el contrato clasificado remita a las normas mínimas sobre seguridad industrial establecidas en el capítulo 6 de la Decisión (UE, Euratom) 2015/444, en las presentes normas de desarrollo y, en su caso, en el anuncio de contrato o en la invitación a presentar ofertas, y de que estas normas se cumplan durante la ejecución.

2. A tal fin, el ordenador competente solicitará, en todas las fases, el dictamen de la autoridad de seguridad de la Comisión sobre cuestiones relativas a los elementos de seguridad de un contrato, programa o proyecto clasificado, e informará al responsable local de seguridad acerca de los contratos celebrados. La decisión sobre el grado de clasificación de temas específicos corresponderá al órgano de contratación y se tomará teniendo debidamente en cuenta la Guía de clasificación de seguridad.

3. Desde el respeto de los requisitos de las presentes normas de desarrollo, la autoridad de seguridad de la Comisión colaborará con las autoridades nacionales de seguridad («ANS») y las autoridades de seguridad designadas («ASD») de los Estados miembros en cuestión, en particular en lo que se refiere a las habilitaciones de seguridad de establecimiento («HSE»), las habilitaciones personales de seguridad («HPS»), los procedimientos de visita y los planes de transporte.

CAPÍTULO 2

GESTIÓN DE LICITACIONES DE CONTRATOS CLASIFICADOS

Artículo 3

Principios básicos

1. Solo se adjudicarán contratos clasificados a operadores económicos registrados en un Estado miembro o a operadores económicos registrados en un tercer país o creados por una organización internacional cuando dicho tercer país u organización internacional haya celebrado un acuerdo sobre seguridad de la información con la Unión Europea o suscrito un acuerdo administrativo con la Comisión ([9]).

2. Antes de la invitación a presentar ofertas para un contrato clasificado, el órgano de contratación determinará la clasificación de seguridad de toda la información que pueda acabar proporcionándose a los licitadores. El órgano de contratación determinará asimismo la clasificación de seguridad máxima de la posible información generada durante la ejecución del contrato, programa o proyecto, o, como mínimo, el volumen y el tipo de información que se prevé que se producirá o manejará, y el grado de necesidad de un sistema de información y comunicaciones («SIC») clasificados.

([8]) 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, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1).

([9]) En el sitio web de la Comisión puede consultarse la lista de acuerdos celebrados por la UE y de acuerdos administrativos suscritos por la Comisión Europea en virtud de los cuales puede intercambiarse información clasificada de la UE con terceros países y organizaciones internacionales.

3. El órgano de contratación se asegurará de que los anuncios de los contratos clasificados proporcionen información sobre las obligaciones especiales en materia de seguridad relacionadas con la información clasificada. En el anexo I figura un ejemplo de modelo de anuncio de contrato.

4. El órgano de contratación se asegurará de que la información clasificada de grado RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se ponga en conocimiento de los licitadores únicamente después de que estos hayan firmado un acuerdo de confidencialidad que los obligue a manejar y proteger la ICUE de conformidad con la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo.

5. Todos los contratistas que deban manejar o almacenar información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en sus instalaciones, ya sea durante la ejecución del propio contrato clasificado o durante la fase precontractual, deberán disponer de una HSE del grado exigido. A continuación, se especifican los tres supuestos que pueden darse durante la fase de licitación de un contrato clasificado que incluya ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

a) No se concede acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante la fase de licitación:

   Cuando el anuncio de contrato o la invitación a presentar ofertas se refiera a un contrato que incluirá ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, pero no requiera que el licitador maneje dicha información en la fase de licitación, los licitadores que no dispongan de una HSE del grado exigido no serán excluidos del proceso de licitación por ese motivo.

b) Se concede acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en los locales del órgano de contratación durante la fase de licitación:

   Se concederá acceso al personal del licitador que esté en posesión de una HPS del grado exigido y que tenga necesidad de conocer. Antes de conceder dicho acceso, el órgano de contratación verificará, a través de la autoridad de seguridad de la Comisión y con las respectivas ANS y ASD si, en esta fase, también es necesaria una HSE en virtud de las disposiciones legales y reglamentarias nacionales.

c) Se maneja o almacena ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en los locales del licitador durante la fase de licitación:

   Cuando el anuncio de contrato o la invitación a presentar ofertas requieran que los licitadores manejen o almacenen ICUE en sus locales, el licitador deberá disponer de una HSE del grado exigido. En tales circunstancias, el órgano de contratación obtendrá, a través de la autoridad de seguridad de la Comisión, una garantía de la ANS o ASD correspondiente de que al licitador se le ha concedido una HSE adecuada. Se concederá acceso al personal del licitador que esté en posesión de una HPS del grado exigido y que tenga necesidad de conocer.

6. En principio, no se exigirá una HSE para acceder a información de grado RESTREINT UE/EU RESTRICTED, ya sea en la fase de licitación o para la ejecución del contrato. Cuando los Estados miembros exijan una HSE para los contratos o subcontratos de grado RESTREINT UE/EU RESTRICTED en virtud de sus disposiciones legales y reglamentarias nacionales, que se enumeran en el anexo IV, dichos requisitos nacionales no podrán imponer obligaciones adicionales a los demás Estados miembros o excluir a los licitadores, contratistas o subcontratistas de los Estados miembros que no dispongan de tales requisitos de HSE para el acceso a información de grado RESTREINT UE/EU RESTRICTED de los contratos o subcontratos correspondientes o de competir para que se les adjudiquen. Estos contratos se ejecutarán en los Estados miembros de conformidad con sus disposiciones legales y reglamentarias nacionales.

7. Cuando se requiera una HSE para la ejecución de un contrato clasificado, el órgano de contratación presentará, a través de la autoridad de seguridad de la Comisión, una solicitud a la ANS o ASD del contratista utilizando una ficha de información sobre la habilitación de seguridad de establecimiento («FIHSE»). El anexo III, apéndice D, contiene un ejemplo de FIHSE ([10]). El contrato clasificado no se adjudicará hasta que la ANS o ASD del contratista haya confirmado la HSE del licitador. La respuesta a una FIHSE se proporcionará, en la medida de lo posible, en un plazo de diez días laborables a partir de la fecha de la solicitud.

([10]) Los formularios que se empleen podrán diferir en su diseño del ejemplo que figura en las presentes normas de desarrollo.

Artículo 4

Subcontratación de contratos clasificados

1. Las condiciones con arreglo a las que un contratista adjudicatario de un contrato clasificado de la Comisión podrá subcontratar deberán definirse en la invitación a presentar ofertas y en la documentación del contrato. Cuando el contrato clasificado permita la subcontratación de algunas de sus partes, dicha subcontratación estará sujeta a que el órgano de contratación otorgue previamente su consentimiento por escrito. Antes de otorgar su consentimiento, el órgano de contratación consultará a la autoridad de seguridad de la Comisión.

2. Únicamente se podrán subcontratar contratos clasificados con operadores económicos registrados en un Estado miembro o con operadores económicos registrados en un tercer país o creados por una organización internacional cuando dicho tercer país u organización internacional haya celebrado un acuerdo sobre seguridad de la información con la Unión Europea o suscrito un acuerdo administrativo con la Comisión ([11]).

CAPÍTULO 3

ADJUDICACIÓN DE CONTRATOS CLASIFICADOS DE LA COMISIÓN

Artículo 5

Principios básicos

1. Al adjudicar un contrato clasificado, el órgano de contratación, junto con la autoridad de seguridad de la Comisión, se asegurará de que las obligaciones del contratista relativas a la protección de la ICUE proporcionada a dicho contratista o generada durante la ejecución del contrato formen parte de este. Los requisitos de seguridad específicos del contrato se describirán en la cláusula sobre aspectos de la seguridad («CAS»). En el anexo III figura un ejemplo de modelo de CAS.

2. Antes de firmar un contrato clasificado, el órgano de contratación elaborará, previa consulta a la autoridad de seguridad de la Comisión, una guía de clasificación de seguridad («GCS») para las tareas que deberán realizarse y la información generada durante la ejecución del contrato o, en su caso, a nivel de programa o proyecto. La CAS incluirá la GCS.

3. Los requisitos de seguridad específicos del programa o proyecto se describirán en las instrucciones de seguridad del programa (o proyecto) («ISP»). Las ISP podrán redactarse utilizando las disposiciones del modelo de CAS que figura en el anexo III. El servicio de la Comisión que gestione el programa o proyecto elaborará, con la colaboración de la autoridad de seguridad de la Comisión, las ISP, que se someterán al dictamen del grupo de expertos en seguridad de la Comisión. Cuando un contrato sea parte de un programa o proyecto que tenga sus propias ISP, la CAS del contrato tendrá una forma simplificada e incluirá una referencia a las disposiciones en materia de seguridad establecidas en las ISP del programa o proyecto.

4. El órgano de contratación tendrá la consideración de originador de la información clasificada producida y manejada para la ejecución del contrato.

5. El órgano de contratación notificará, a través de la autoridad de seguridad de la Comisión, a las ANS o ASD de todos los contratistas y subcontratistas la celebración de contratos o subcontratos clasificados y los casos de extinción anticipada o las prórrogas de dichos contratos o subcontratos. En el anexo IV figura una lista de requisitos por países.

6. Los contratos que incluyan información clasificada de grado RESTREINT UE/EU RESTRICTED incluirán una cláusula de seguridad que haga vinculantes para el contratista las disposiciones del anexo III, apéndice E. Estos contratos incluirán una CAS en la que se indiquen, como mínimo, los requisitos de manejo de información de grado RESTREINT UE/EU RESTRICTED, en particular los aspectos de garantía de la información y los requisitos específicos que debe cumplir el contratista que haya recibido una delegación del órgano de contratación para la acreditación del SIC del contratista que maneje la información de grado RESTREINT UE/EU RESTRICTED.

([11]) En el sitio web de la Comisión puede consultarse la lista de acuerdos celebrados por la UE y de acuerdos administrativos suscritos por la Comisión Europea en virtud de los cuales puede intercambiarse información clasificada de la UE con terceros países y organizaciones internacionales.

7. Cuando se proporcione información de grado RESTREINT UE/EU RESTRICTED a los licitadores o a posibles contratistas, los requisitos mínimos mencionados en el apartado 6 se incluirán en las ofertas o en los acuerdos de confidencialidad pertinentes celebrados durante la fase de licitación.

8. Cuando así lo exijan las disposiciones legales y reglamentarias de los Estados miembros, las ANS o ASD se asegurarán de que los contratistas o subcontratistas del ámbito de su competencia cumplan las disposiciones de seguridad aplicables para la protección de la información de grado RESTREINT UE/EU RESTRICTED y realicen visitas de verificación a las instalaciones de los contratistas situadas en su territorio. Cuando la ANS o ASD no esté sujeta a dicha obligación, el órgano de contratación se asegurará de que el contratista aplique las disposiciones de seguridad exigidas según lo dispuesto en el anexo III.

Artículo 6

Acceso del personal de los contratistas y subcontratistas a ICUE

1. El servicio de la Comisión correspondiente, en su calidad de órgano de contratación, se asegurará de que los contratos clasificados contengan disposiciones que indiquen que al personal del contratista o subcontratista que necesite acceder a ICUE para la ejecución del contrato o subcontrato clasificado solo se le concederá dicho acceso si:

a) se ha corroborado que tiene necesidad de conocer;

b) la ANS o ASD correspondiente o cualquier otra autoridad de seguridad competente le ha concedido una HPS del grado correspondiente en relación con información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET;

c) ha sido instruido sobre las normas de seguridad aplicables para la protección de la ICUE y ha aceptado sus responsabilidades en lo que respecta a la protección de dicha información.

2. Si un contratista o subcontratista desea emplear a un nacional de un tercer país en un puesto que requiera el acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, será responsabilidad del contratista o subcontratista iniciar el procedimiento de habilitación de seguridad de dicha persona, de conformidad con las disposiciones legales y reglamentarias nacionales aplicables en el lugar en que vaya a concederse el acceso a la ICUE.

CAPÍTULO 4

VISITAS EN RELACIÓN CON CONTRATOS CLASIFICADOS

Artículo 7

Principios básicos

1. Cuando la Comisión, los contratistas o los subcontratistas necesiten acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET que se halle en los locales de otra de las partes para la ejecución de un contrato clasificado, se organizarán visitas, con la colaboración de las ANS, las ASD o cualquier otra autoridad de seguridad competente.

2. Las visitas a que se refiere el apartado 1 estarán sujetas a los requisitos siguientes:

a) la visita tendrá una finalidad oficial relacionada con un contrato clasificado adjudicado por la Comisión;

b) todos los visitantes deberán estar en posesión de una HPS del grado exigido y tener necesidad de conocer para acceder a ICUE proporcionada o generada durante la ejecución de un contrato clasificado adjudicado por la Comisión.

Artículo 8

Solicitudes de visita

1. Las visitas de contratistas a las instalaciones de otros contratistas o a los locales de la Comisión que impliquen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se organizarán con arreglo al procedimiento siguiente:

a) El responsable de seguridad de la instalación que envía al visitante cumplimentará todas las partes pertinentes del formulario de solicitud de visita («SdV») y presentará la solicitud a la ANS o ASD de la instalación. En el anexo III, apéndice C, figura un modelo de SdV.

b) La ANS o ASD de la instalación que envía al visitante debe confirmar la HPS del visitante antes de presentar la SdV a la ANS o ASD de la instalación que lo recibe (o a la autoridad de seguridad de la Comisión si la visita se realiza en los locales de la Comisión).

c) El responsable de seguridad de la instalación que envía al visitante recibirá entonces de su ANS o ASD la respuesta de la ANS o ASD de la instalación que lo recibe (o de la autoridad de seguridad de la Comisión) por la que se autorice o deniegue la SdV.

d) Una SdV se considerará aprobada si no se presentan objeciones hasta cinco días laborables antes de la fecha de la visita.

2. Las visitas de los funcionarios de la Comisión a las instalaciones del contratista que impliquen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se organizarán con arreglo al procedimiento siguiente:

a) El visitante cumplimentará todas las partes pertinentes de la SdV y la presentará a la autoridad de seguridad de la Comisión.

b) La autoridad de seguridad de la Comisión confirmará la HPS del visitante antes de remitir la SdV a la ANS o ASD de la instalación que lo recibe.

c) La autoridad de seguridad de la Comisión recibirá una respuesta de la ANS o ASD de la instalación que recibe la vista por la que se autorice o deniegue la SdV.

d) Una SdV se considerará aprobada si no se presentan objeciones hasta cinco días laborables antes de la fecha de la visita.

3. Una SdV puede abarcar una única visita o visitas periódicas. En caso de visitas periódicas, la SdV podrá tener una validez máxima de un año a partir de la fecha de inicio solicitada.

4. La validez de una SdV no excederá la validez de la HPS del visitante.

5. Por regla general, las SdV deben presentarse a la autoridad de seguridad competente de la instalación que recibe la vista al menos quince días laborables antes de la fecha de esta.

Artículo 9

Procedimientos de visita

1. Antes de permitir que los visitantes tengan acceso a ICUE, el responsable de seguridad de la instalación que recibe la visita deberá cumplir todos los procedimientos y normas de seguridad en materia de visitas establecidos por su ANS o ASD.

2. Los visitantes acreditarán su identidad al llegar a la instalación que los recibirá presentando un documento de identidad o pasaporte válido. Dicha información de identificación se corresponderá con la información proporcionada en la SdV.

3. La instalación que recibe la visita se asegurará de que se lleve un registro de todos los visitantes, incluidos sus nombres y apellidos, la organización a la que representan, la fecha de caducidad de la HPS, la fecha de la visita y los nombres y apellidos de las personas visitadas. Este registro se conservará durante un período mínimo de cinco años, o más si así lo exigen las disposiciones normativas y reglamentarias del país en el que se encuentre la instalación que recibe la visita.

Artículo 10

Visitas organizadas directamente

1. Cuando se trate de proyectos específicos, las ANS o ASD pertinentes y la autoridad de seguridad de la Comisión podrán acordar un procedimiento por el que las visitas relativas a contratos clasificados específicos puedan ser organizadas directamente por el responsable de seguridad del visitante y el responsable de seguridad de la instalación que se vaya a visitar. En el anexo III, apéndice C, figura una modelo del formulario que debe utilizarse a tal fin. Dicho procedimiento excepcional se recogerá en las ISP o en otros acuerdos específicos. En estos supuestos, no serán de aplicación los procedimientos establecidos en el artículo 8 y el artículo 9, apartado 1.

2. Las visitas que impliquen el acceso a información clasificada de grado RESTREINT UE/EU RESTRICTED serán organizadas directamente por la entidad que envía al visitante y la que lo recibe sin necesidad de seguir los procedimientos establecidos en el artículo 8 y el artículo 9, apartado 1.

CAPÍTULO 5

TRANSMISIÓN Y TRANSPORTE DE ICUE PARA LA EJECUCIÓN DE CONTRATOS CLASIFICADOS

Artículo 11

Principios básicos

El órgano de contratación se asegurará de que todas las decisiones relativas a la transmisión y el transporte de ICUE se ajusten a la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo, así como a las cláusulas del contrato clasificado, incluido el consentimiento del originador.

Artículo 12

Manejo electrónico

1. El manejo y la transmisión electrónicos de ICUE se realizarán de conformidad con los capítulos 5 y 6 de la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo.

Los sistemas de información y comunicaciones que sean propiedad de un contratista y se utilicen para manejar la ICUE necesaria para la ejecución del contrato («SIC del contratista») tendrán que ser acreditados por la autoridad de acreditación de seguridad («AAS») competente. Toda transmisión electrónica de ICUE se protegerá con productos criptológicos aprobados de conformidad con el artículo 36, apartado 4, de la Decisión (UE, Euratom) 2015/444. Las medidas TEMPEST se ejecutarán de conformidad con el artículo 36, apartado 6, de dicha Decisión.

2. La acreditación de seguridad del SIC del contratista que maneje ICUE de grado RESTREINT UE/EU RESTRICTED y cualquier interconexión de este podrán delegarse en el responsable de seguridad del contratista si así lo permiten las disposiciones legales y reglamentarias nacionales. Cuando esta tarea sea delegada, el contratista será responsable de respetar los requisitos mínimos de seguridad descritos en la CAS al manejar información de grado RESTREINT UE/EU RESTRICTED en su SIC. Sin embargo, las ANS, las ASD y las AAS pertinentes siguen siendo responsables de la protección de la información de grado RESTREINT UE/EU RESTRICTED que manejen los contratistas y siguen gozando de la facultad de examinar las medidas de seguridad adoptadas por los contratistas. Además, el contratista remitirá al órgano de contratación y, cuando así lo exijan las disposiciones legales y reglamentarias nacionales, a la AAS nacional competente una declaración de conformidad que certifique que el SIC del contratista y las interconexiones correspondientes han sido acreditados para el manejo de ICUE de grado RESTREINT UE/EU RESTRICTED ([12]).

Artículo 13

Transporte por medio de mensajero comercial

El transporte de ICUE por medio de mensajero comercial cumplirá las disposiciones pertinentes de las decisiones de la Comisión relativas a las normas de desarrollo para el manejo de información de grado RESTREINT UE/EU RESTRICTED y CONFIDENTIEL UE/EU CONFIDENTIAL.

Artículo 14

Transporte en mano

1. El transporte en mano de información clasificada está sujeto a requisitos estrictos de seguridad.

2. La información de grado RESTREINT UE/EU RESTRICTED podrá ser transportada en mano por el personal del contratista dentro de la UE siempre que se cumplan los siguientes requisitos:

a) que el sobre o empaquetado utilizado sea opaco y no indique la clasificación de su contenido;

([12]) Los requisitos mínimos aplicables a los sistemas de información y comunicaciones que manejen ICUE de grado RESTREINT UE/EU RESTRICTED se establecen en el anexo III, apéndice E.

b) que la información clasificada esté en todo momento en posesión del portador;

c) que el sobre o empaquetado no se abra en tránsito.

3. En el caso de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, el transporte en mano por parte del personal del contratista dentro de un Estado miembro de la UE será organizado por adelantado por las entidades de origen y de destino. La autoridad o instalación emisora informará a la autoridad o instalación receptora de los datos del envío, incluidos la referencia, la clasificación, la hora prevista de llegada y el nombre del mensajero. Este transporte en mano se permite siempre que se cumplan los siguientes requisitos:

a) que la información clasificada se transporte en un sobre o empaquetado doble;

b) que el sobre o empaquetado exterior esté protegido y no indique la clasificación de su contenido, pero que el sobre interior sí indique el grado de clasificación;

c) que la ICUE esté en todo momento en posesión del portador;

d) que el sobre o empaquetado no se abra en tránsito;

e) que el sobre o empaquetado se transporte en un maletín con cerradura o en un objeto homologado similar del mismo tamaño y peso que el portador pueda llevar consigo en todo momento y que no haya que facturar como equipaje;

f) que el mensajero lleve un certificado de correo expedido por su autoridad de seguridad competente por el que se le autorice a transportar el envío clasificado de que se trate.

4. Para el transporte en mano de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET de un Estado miembro de la UE a otro por parte del personal del contratista, se aplicarán las siguientes normas adicionales:

a) el mensajero será responsable de la custodia del material clasificado hasta su entrega al destinatario;

b) en caso de fallo de seguridad, la ANS o ASD del remitente podrá solicitar que las autoridades del país en que se haya producido el fallo lleven a cabo una investigación, comuniquen sus conclusiones y emprendan acciones legales o de otro tipo, según proceda;

c) el mensajero deberá ser informado de todas las obligaciones en materia de seguridad que deben observarse durante el transporte y deberá firmar una declaración de reconocimiento de tales obligaciones;

d) las instrucciones para el mensajero se adjuntarán al certificado de correo;

e) el mensajero deberá disponer de una descripción del envío y un itinerario;

f) los documentos se devolverán a la ANS o ASD emisora al finalizar el trayecto o trayectos, o el destinatario los conservará a efectos de controles ulteriores;

g) si las autoridades aduaneras, las autoridades de inmigración o la policía de fronteras solicitan examinar e inspeccionar el envío, se les permitirá abrir y observar suficientes partes del envío como para cerciorarse de que no contienen ningún material distinto del declarado;

h) debe instarse a las autoridades aduaneras a que respeten la autoridad oficial de los documentos enviados y los documentos de autorización transportados por el mensajero.

Si las autoridades aduaneras abren un envío, deberá hacerse fuera de la vista de las personas no autorizadas y en presencia del mensajero cuando sea posible. El mensajero solicitará que se vuelva a empaquetar el envío y pedirá a las autoridades que lleven a cabo la inspección que vuelvan a precintar el envío y que confirmen por escrito que lo han abierto.

5. El transporte en mano de información clasificada de grado RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET por parte del personal del contratista a un tercer país o a una organización internacional estará sujeto a las disposiciones del acuerdo sobre seguridad de la información o del acuerdo administrativo celebrado entre, respectivamente, la Unión Europea o la Comisión y dicho tercer país u organización internacional.

CAPÍTULO 6

PLAN DE CONTINUIDAD DE LA ACTIVIDAD

Artículo 15

Planes de contingencia y medidas de recuperación

El servicio de la Comisión correspondiente, en su calidad de órgano de contratación, se asegurará de que el contrato clasificado obligue al contratista a establecer planes de contingencia para proteger, en situaciones de emergencia, la ICUE manejada para la ejecución del contrato clasificado, y a establecer medidas preventivas y de recuperación en el contexto de la planificación de la continuidad de la actividad a fin de minimizar el efecto de los incidentes relacionados con el manejo y el almacenamiento de la ICUE. El contratista informará al órgano de contratación de su plan de contingencia.

Artículo 16

Entrada en vigor

La presente Decisión entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 17 de octubre de 2019.

Por la Comisión,

en nombre del Presidente,

Günther H. OETTINGER

Miembro de la Comisión

ANEXO I

INFORMACIÓN ESTÁNDAR DE LOS ANUNCIOS DE CONTRATOS PÚBLICOS

(adáptese a los anuncios de contratos utilizados)

Para los contratos cuya ejecución afecte a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET

Otras condiciones particulares (*en su caso*)

La ejecución del contrato está sujeta a condiciones particulares ● sí ○ no

(*en caso de respuesta afirmativa*) Descripción de las condiciones particulares:

El contrato implicará el acceso, manejo y/o almacenamiento de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, que está sujeta a las normas de seguridad para la protección de la información clasificada de la UE establecidas en la Decisión (UE, Euratom) 2015/444 de la Comisión, y a las normas de desarrollo de dicha Decisión ([1]).

Se exigirá una habilitación de seguridad de establecimiento, así como habilitaciones personales de seguridad para el personal del contratista que maneje información clasificada.

Las obligaciones especiales en materia de seguridad formarán parte del contrato (cláusula sobre aspectos de la seguridad, adjunta al contrato). La subcontratación estará sujeta a la aprobación previa por escrito del órgano de contratación y al cumplimiento de todas las normas de seguridad por parte del subcontratista y su personal.

Para los contratos cuya ejecución afecte a información clasificada de grado RESTREINT UE/EU RESTRICTED

Otras condiciones particulares (*en su caso*)

La ejecución del contrato está sujeta a condiciones particulares ● sí ○ no

(*en caso de respuesta afirmativa*) Descripción de las condiciones particulares:

El contrato implicará el acceso, manejo y/o almacenamiento de información clasificada de grado RESTREINT UE/EU RESTRICTED, que está sujeta a las normas de seguridad para la protección de la información clasificada de la UE establecidas en la Decisión (UE, Euratom) 2015/444, y a las normas de desarrollo de dicha Decisión ([2]).

Las obligaciones especiales en materia de seguridad formarán parte del contrato (cláusula sobre aspectos de la seguridad, adjunta al contrato). La subcontratación estará sujeta a la aprobación previa por escrito del órgano de contratación y al cumplimiento de todas las normas de seguridad por parte del subcontratista y su personal.

([1]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.
([2]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

ANEXO II

CLÁUSULAS CONTRACTUALES TIPO

(adáptese a los contratos utilizados)

ARTÍCULO XX

OBLIGACIONES EN MATERIA DE SEGURIDAD

XX.1. Información clasificada de la UE

Si la ejecución del contrato implica el uso o generación de información clasificada de la UE, dicha información debe tratarse de acuerdo con la cláusula sobre aspectos de la seguridad («CAS») y su guía de clasificación de seguridad («GCS»), que figuran en el anexo 1, y la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo ([1]), hasta que se desclasifique.

Todos los entregables que contengan información clasificada deben enviarse con arreglo a procedimientos especiales acordados con el órgano de contratación.

Las tareas de la acción relacionadas con información clasificada no pueden subcontratarse sin la aprobación previa, expresa y por escrito del órgano de contratación.

No puede revelarse información clasificada de la UE a ningún tercero (incluidos los subcontratistas) sin la aprobación previa, expresa y por escrito del órgano de contratación.

([1]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

ANEXO III

[anexo IV (del contrato marco)]

CLÁUSULA SOBRE ASPECTOS DE LA SEGURIDAD

[Modelo]

Apéndice A

REQUISITOS DE SEGURIDAD

El órgano de contratación debe incluir los siguientes requisitos de seguridad en la cláusula sobre aspectos de la seguridad. Es posible que algunas cláusulas no se apliquen al contrato; se muestran entre corchetes.

La lista de cláusulas no es exhaustiva. Podrán añadirse cláusulas adicionales dependiendo de la naturaleza del contrato clasificado.

CONDICIONES GENERALES

[*N.B.: aplicable a todos los contratos clasificados*]

1. La presente cláusula sobre aspectos de la seguridad («CAS») forma parte del contrato [o subcontrato] clasificado y describe los requisitos de seguridad específicos del contrato. El incumplimiento de estos requisitos puede ser motivo suficiente para resolver el contrato.

2. Los contratistas están sujetos a todas las obligaciones establecidas en la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo ([1]).

3. La información clasificada generada durante la ejecución del contrato debe estar marcada como información clasificada de la UE («ICUE») con el grado de clasificación de seguridad correspondiente con arreglo a lo determinado en la guía de clasificación de seguridad («GCS») que figura en el apéndice B de la presente cláusula. Solo se podrá emplear un grado de clasificación de seguridad distinto al fijado por la GCS si media la autorización escrita del órgano de contratación.

4. Los derechos del originador de cualquier ICUE producida y manejada para la ejecución del contrato clasificado serán ejercidos por la Comisión, en su calidad de órgano de contratación.

5. Sin el consentimiento por escrito del órgano de contratación, el contratista o subcontratista no podrá utilizar la información o el material proporcionados por el órgano de contratación o producidos en su nombre para ningún fin distinto del contrato.

6. El contratista debe investigar todos los fallos de seguridad relacionados con la ICUE y notificarlos al órgano de contratación tan pronto como sea posible. El contratista o subcontratista debe informar de inmediato a la autoridad nacional de seguridad («ANS») competente o a la autoridad de seguridad designada («ASD») y, si lo permiten las disposiciones legales y reglamentarias nacionales, a la autoridad de seguridad de la Comisión, sobre todos los casos en que se conozca, o existan razones para sospechar, que la ICUE proporcionada o generada con arreglo al contrato se ha perdido o ha acabado en conocimiento de personas no autorizadas.

7. Al finalizar el contrato, el contratista o subcontratista debe devolver cualquier ICUE que obre en su poder al órgano de contratación a la mayor brevedad. Cuando sea posible, el contratista o subcontratista puede destruir la ICUE en lugar de devolverla. Esto debe hacerse con arreglo a las disposiciones legales y reglamentarias del país en que esté establecido el contratista, previo consentimiento de la autoridad de seguridad de la Comisión y siguiendo las instrucciones de esta última. La ICUE debe destruirse de tal forma que no pueda reconstruirse, ya sea en todo o en parte.

8. Cuando el contratista o subcontratista esté autorizado a conservar la ICUE tras resolverse o finalizar el contrato, la ICUE debe seguir protegiéndose de conformidad con la Decisión (UE, Euratom) 2015/444 («DC 2015/444»), y con sus normas de desarrollo ([2]).

9. Todo manejo, tratamiento y transmisión electrónicos de la ICUE debe respetar lo dispuesto en los capítulos 5 y 6 de la DC 2015/444. Algunos de los aspectos que se regulan en dichos capítulos son: el requisito de que los sistemas de información y comunicaciones que sean de propiedad del contratista y se utilicen para manejar la ICUE a efectos del contrato («SIC del contratista») se acrediten ([3]); la obligación de que toda transmisión electrónica de ICUE se proteja por medio de productos criptológicos aprobados de conformidad con el artículo 36, apartado 4, de la DC 2015/444; y la obligación de ejecutar las medidas TEMPEST de conformidad con el artículo 36, apartado 6, de la DC 2015/444.

([1]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.
([2]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.
([3]) La parte que desee la acreditación deberá remitir al órgano de contratación una declaración de conformidad, a través de la autoridad de seguridad de la Comisión, y con la colaboración de la autoridad de acreditación de seguridad («AAS») nacional pertinente.

10. El contratista o subcontratista debe contar con planes de contingencia para proteger, en situaciones de emergencia, cualquier ICUE manejada durante la ejecución del contrato clasificado y debe adoptar medidas preventivas y de recuperación para minimizar el efecto de los incidentes relacionados con el manejo y el almacenamiento de la ICUE. El contratista o subcontratista debe informar al órgano de contratación de su plan de contingencia.

CONTRATOS QUE PRECISAN ACCESO A INFORMACIÓN CLASIFICADA DE GRADO RESTREINT UE/EU RESTRICTED

11. No es necesario contar con una habilitación personal de seguridad («HPS»). No obstante, solo puede acceder a la información o el material clasificado de grado RESTREINT UE/EU RESTRICTED el personal del contratista que necesite dicha información para ejecutar el contrato (*principio de la necesidad de conocer*), que haya sido informado por el responsable de seguridad del contratista sobre sus responsabilidades y sobre las consecuencias de cualquier comprometimiento o fallo de la seguridad de dicha información, y que haya declarado por escrito que tiene conocimiento de las consecuencias de incumplir la obligación de proteger la ICUE.

12. Salvo que el órgano de contratación dé su consentimiento por escrito, el contratista o subcontratista no puede dar acceso a información o material clasificados de grado RESTREINT UE/EU RESTRICTED a entidades o personas distintas de aquellos miembros de su personal que tengan necesidad de conocer.

13. El contratista o subcontratista debe mantener las marcas de clasificación de seguridad de la información clasificada generada o proporcionada durante la ejecución del contrato y no puede desclasificarla sin la autorización por escrito del órgano de contratación.

14. La información o el material clasificados de grado RESTREINT UE/EU RESTRICTED debe almacenarse en mobiliario de oficina con cerradura cuando no se use. Cuando se encuentren en tránsito, los documentos deben transportarse dentro de un sobre opaco. Los documentos deben estar en todo momento en posesión del portador y no abrirse en tránsito.

15. El contratista o subcontratista puede entregar a la Comisión documentos clasificados de grado RESTREINT UE/EU RESTRICTED en mano, por medios electrónicos o por medio de servicios de mensajería comercial o de correos. Para ello, el contratista o subcontratista debe seguir las instrucciones de seguridad del programa (o proyecto) («ISP») de la Comisión y las normas de desarrollo de la Comisión sobre la seguridad industrial en relación con los contratos públicos clasificados ([4]).

16. Cuando dejen de ser necesarios, los documentos clasificados de grado RESTREINT UE/EU RESTRICTED deben destruirse de tal forma que no puedan reconstruirse, ya sea en todo o en parte.

17. La acreditación de seguridad del SIC del contratista que maneje ICUE de grado RESTREINT UE/EU RESTRICTED y cualquier interconexión de este podrán delegarse en el responsable de seguridad del contratista si así lo permiten las disposiciones legales y reglamentarias nacionales. Cuando se delegue la acreditación, las ANS, las ASD y las AAS seguirán siendo responsables de la protección de la información de grado RESTREINT UE/EU RESTRICTED que manejen los contratistas y seguirán gozando de la facultad de examinar las medidas de seguridad adoptadas por el contratista. Además, el contratista remitirá al órgano de contratación y, cuando así lo exijan las disposiciones legales y reglamentarias nacionales, a la AAS nacional competente una declaración de conformidad que certifique que el SIC del contratista y las interconexiones correspondientes han sido acreditados para el manejo de ICUE de grado RESTREINT UE/EU RESTRICTED.

MANEJO DE INFORMACIÓN CLASIFICADA DE GRADO RESTREINT UE/EU RESTRICTED EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

18. En el apéndice E de la presente CAS figuran los requisitos mínimos de los SIC que manejan información clasificada de grado RESTREINT UE/EU RESTRICTED.

CONDICIONES EN QUE EL CONTRATISTA PUEDE SUBCONTRATAR

19. El contratista debe solicitar el permiso del servicio de la Comisión correspondiente, en su calidad de órgano de contratación, antes de subcontratar cualquier parte de un contrato clasificado.

([4]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

20. No se podrá autorizar la subcontratación a una empresa registrada en un Estado que no sea miembro de la UE ni a una entidad perteneciente a una organización internacional si dicho Estado no perteneciente a la UE o dicha organización internacional no ha celebrado un acuerdo sobre seguridad de la información con la Unión Europea o un acuerdo administrativo con la Comisión.

21. Cuando el contratista subcontrate, las disposiciones de seguridad del contrato serán de aplicación *mutatis mutandis* al subcontratista o subcontratistas y a su personal. En tal caso, corresponde al contratista asegurarse de que todos los subcontratistas apliquen estos principios a sus propios acuerdos de subcontratación. Para garantizar una supervisión adecuada de la seguridad, se deberá notificar a la ANS o ASD del contratista o subcontratista la subcontratación de todos los contratos clasificados conexos de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET. Cuando proceda, se deberá entregar a las ANS o ASD del contratista o subcontratista una copia de las disposiciones de seguridad específicas del subcontrato. En el anexo de las normas de desarrollo de la Comisión sobre la seguridad industrial en relación con los contratos públicos clasificados ([1]) figuran las ANS o ASD que exigen que se les notifiquen las disposiciones de seguridad de los contratos clasificados de grado RESTREINT UE/EU RESTRICTED.

22. El contratista no puede revelar ICUE a un subcontratista sin la aprobación previa por escrito del órgano de contratación. Si la ICUE debe enviarse a los subcontratistas con frecuencia o de manera rutinaria, el órgano de contratación puede dar su aprobación para un período de tiempo determinado (por ejemplo, doce meses) o para la duración del subcontrato.

VISITAS

Si se aplica el procedimiento de SdV estándar a visitas que impliquen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el órgano de contratación debe incluir los apartados 23, 24 y 25 y suprimir el apartado 26. Si el establecimiento que envía al visitante y el que lo recibe organizan directamente las visitas que impliquen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el órgano de contratación debe suprimir los apartados 24 y 25 e incluir únicamente el apartado 26.

23. Las visitas que impliquen el acceso, o posible acceso, a información clasificada de grado RESTREINT UE/EU RESTRICTED serán organizadas directamente por el establecimiento que envía al visitante y el que lo recibe sin necesidad de seguir el procedimiento descrito en los apartados 24 a 26.

[24. Las visitas que impliquen el acceso, o posible acceso, a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se regirán por el procedimiento siguiente:

a) El responsable de seguridad de la instalación que envía al visitante cumplimentará todas las partes pertinentes del formulario SdV (apéndice C) y presentará la solicitud a la ANS o ASD de la instalación.

b) La ANS o ASD de la instalación que envía al visitante debe confirmar la HPS del visitante antes de presentar la SdV a la ANS o ASD de la instalación que lo recibe (o a la autoridad de seguridad de la Comisión si la visita se realiza en los locales de la Comisión).

c) El responsable de seguridad de la instalación que envía al visitante recibirá entonces de su ANS o ASD la respuesta de la ANS o ASD de la instalación que lo recibe (o de la autoridad de seguridad de la Comisión) por la que se autorice o deniegue la SdV.

d) Una SdV se considerará aprobada si no se presentan objeciones hasta cinco días laborables antes de la fecha de la visita.]

[25. Antes de dar al visitante o visitantes acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, la instalación que los reciba debe haber recibido la autorización de su ANS o ASD.]

[26. Las visitas que impliquen el acceso, o posible acceso, a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET serán organizadas directamente por el establecimiento que envía al visitante y el que lo recibe (un ejemplo del formulario que puede utilizarse para este fin figura en el apéndice C).]

([1]) El órgano de contratación debe introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

27. Los visitantes deben acreditar su identidad al llegar a la instalación que los reciba presentando un documento de identidad o pasaporte válido.

28. La instalación que reciba la visita debe asegurarse de que se lleve un registro de todos los visitantes. Estos deben incluir sus nombres y apellidos, la organización a la que representan, la fecha de caducidad de la HPS (si procede), la fecha de la visita y los nombres y apellidos de las personas visitadas. Sin perjuicio de las normas europeas de protección de datos, dichos registros deben conservarse durante un período no inferior a cinco años o lo que indiquen las disposiciones legales y reglamentarias nacionales, según proceda.

VISITAS DE EVALUACIÓN

29. La autoridad de seguridad de la Comisión puede, con la colaboración de la ANS o ASD correspondiente, efectuar visitas a las instalaciones de los contratistas o subcontratistas para comprobar que se cumplen los requisitos de seguridad para el manejo de ICUE.

GUÍA DE CLASIFICACIÓN DE SEGURIDAD

30. La guía de clasificación de seguridad («GCS») contiene una lista de todos los elementos del contrato que estén clasificados o puedan clasificarse durante la ejecución del contrato, las normas por las que se rija dicha clasificación y la especificación de los grados de clasificación de seguridad aplicables. La guía de clasificación de seguridad forma parte del presente contrato y se encuentra en el apéndice B del presente anexo.

Apéndice B

GUÍA DE CLASIFICACIÓN DE SEGURIDAD

[adáptense las partes que procedan dependiendo del objeto del contrato]

Apéndice C

SOLICITUD DE VISITA

(MODELO)

Instrucciones pormenorizadas para cumplimentar una solicitud de visita

(la solicitud solo se puede presentar en inglés)

HEADING	Márquense las casillas correspondientes del tipo de visita y tipo de información e indíquense cuántos lugares deben visitarse y el número de visitantes.
4. **ADMINISTRATIVE DATA**	Deben cumplimentarlos la ANS o ASD solicitante.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Indíquense el nombre y la dirección postal completos. Menciónense la localidad, el país y el código postal según proceda.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Indíquense el nombre y la dirección postal completos. Menciónense la localidad, el país, el código postal, el número télex o de fax (si procede), el número de teléfono y el correo electrónico. Indíquense el nombre, los números de teléfono y fax y el correo electrónico de su punto de contacto principal o de la persona con la que haya concertado la visita. Observaciones: 1) Es importante consignar el código postal correcto porque una empresa puede tener varias instalaciones. 2) Al presentar la solicitud en persona, puede utilizarse el anexo 1 cuando se deban visitar dos o más instalaciones en relación con un mismo aspecto. Cuando se utilice un anexo, el apartado 3 debe indicar: «VÉASE EL ANEXO 1, NÚMERO DE INSTALACIONES:…» (indíquese el número de instalaciones).
7. **DATES OF VISIT**	Indíquese la fecha o el período (de fecha a fecha) reales de la visita, en formato «día – mes – año». Cuando proceda, las fechas o períodos alternativos deben mencionarse entre paréntesis.
8. **TYPE OF INITIATIVE**	Especifíquese si la visita se solicita por iniciativa de la organización o la instalación solicitante o por invitación de la instalación que se vaya a visitar.
9. **THE VISIT RELATES TO:**	Especifíquese el nombre completo del proyecto, contrato o licitación utilizando solo abreviaturas de uso común.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Descríbanse brevemente los motivos de la visita. Evítese el uso de abreviaturas no explicadas. Observaciones: En el caso de visitas periódicas, este apartado debe anteponer «Visitas periódicas» a cualquier otro dato (por ejemplo, Visitas periódicas para discutir ___).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Indíquese SECRET UE/EU SECRET (S-UE/EU-S) o CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), según corresponda.
12. **PARTICULARS OF VISITOR**	Observación: cuando en la visita participen más de dos visitantes, debe utilizarse el anexo 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	En este apartado debe incluirse el nombre y apellidos, el número de teléfono, el número de fax y el correo electrónico del responsable de seguridad de la instalación solicitante.
14. **CERTIFICATION OF SECURITY CLEARANCE**	La autoridad de certificación debe cumplimentar esta casilla. Notas para la autoridad de certificación: a) Indíquense el nombre, la dirección, el número de teléfono, el número de fax y el correo electrónico (puede preimprimirse). b) Esta casilla debe firmarse y sellarse (si procede).
15. **REQUESTING SECURITY AUTHORITY**	La ANS o ASD debe cumplimentar esta casilla. Nota para la ANS o ASD: a) Indíquense el nombre, la dirección, el número de teléfono, el número de fax y el correo electrónico (puede preimprimirse). b) Esta casilla debe firmarse y sellarse (si procede).

Deben cumplimentarse todas las casillas y el formulario debe presentarse a través de canales intergubernamentales ([2]).

([2]) Si se ha acordado que las visitas que impliquen el acceso, o posible acceso, a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET pueden organizarse directamente, el formulario cumplimentado puede presentarse directamente al responsable de seguridad del establecimiento que vaya a visitarse.

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Espacio reservado para la referencia a la legislación aplicable en materia de datos personales y el enlace a la información obligatoria para el interesado, por ejemplo, cómo se aplica el artículo 13 del Reglamento general de protección de datos ([3]).>

(3) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

ANEXO 1 del FORMULARIO de SdV

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Espacio reservado para la referencia a la legislación aplicable en materia de datos personales y el enlace a la información obligatoria para el interesado, por ejemplo, cómo se aplica el artículo 13 del Reglamento general de protección de datos ([1]).>

([1]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

ANEXO 2 del FORMULARIO de SdV

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Espacio reservado para la referencia a la legislación aplicable en materia de datos personales y el enlace a la información obligatoria para el interesado, por ejemplo, cómo se aplica el artículo 13 del Reglamento general de protección de datos ([1]).>

([1]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

Apéndice D

FICHA DE INFORMACIÓN SOBRE LA HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO

(MODELO)

1. **Introducción**

1.1. Se adjunta una ficha de información sobre la habilitación de seguridad de establecimiento («FIHSE») para el intercambio rápido de información entre la autoridad nacional de seguridad («ANS») o la autoridad de seguridad designada («ASD»), otras autoridades nacionales de seguridad competentes y la Comisión (en su calidad de órgano de contratación), en relación con la habilitación de seguridad de establecimiento («HSE») de una instalación a la que afecten licitaciones, contratos o subcontratos clasificados.

1.2. La FIHSE solo es válida si cuenta con el sello de la correspondiente ANS o ASD u otra autoridad competente.

1.3. La FIHSE se divide en una sección de solicitud y una de respuesta y puede utilizarse para los fines antes señalados o para cualquier otro fin que requiera la HSE de una instalación determinada. La ANS o ASD debe especificar el motivo de la investigación en el apartado 7 de la sección de solicitud.

1.4. La información que figura en la FIHSE no suele ser clasificada; en consecuencia, cuando la Comisión y las ANS o ASD correspondientes deban enviarse una FIHSE, se deberá hacer preferentemente por medios electrónicos.

1.5. Las ANS o ASD deben hacer todo lo posible por responder a la petición de una FIHSE en un plazo de diez días laborables.

1.6. En caso de que se transmita información clasificada o se adjudique un contrato en relación con esta garantía, se debe informar a la ANS o ASD emisora.

Procedimientos e instrucciones para el uso de la ficha de información sobre la habilitación de seguridad de establecimiento

Estas instrucciones pormenorizadas están dirigidas a la ANS, la ASD o el órgano de contratación de la Comisión que cumplimente el FIHSE. La solicitud debe, preferentemente, mecanografiarse en mayúsculas.

ENCABEZAMIENTO	El solicitante escribe el nombre completo de la ANS o ASD y el nombre del país.
1. **TIPO DE SOLICITUD**	El órgano de contratación solicitante selecciona la casilla apropiada en función del tipo de solicitud de FIHSE. Indíquese el grado de la habilitación de seguridad solicitada. Deben utilizarse las abreviaturas siguientes: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C SIC = Sistemas de información y comunicaciones para el tratamiento de información clasificada

2. **INFORMACIÓN DEL OBJETO**	Los apartados 1 a 6 se explican por sí mismos. En el apartado 4, debe utilizarse el código de dos letras distintivo del país. El apartado 5 es opcional.
3. **MOTIVO DE LA SOLICITUD**	Indíquense el motivo específico de la solicitud y los indicadores del proyecto o el número de contrato o de la invitación a presentar ofertas. Especifíquense la necesidad de capacidad de almacenamiento, el nivel de clasificación del SIC, etc. Deben incluirse todos los plazos, vencimientos y fechas de adjudicación que puedan afectar a una HSE.
4. **ANS O ASD SOLICITANTE**	Indíquense el nombre del solicitante (en nombre de la ANS o ASD) y la fecha de la solicitud en formato numérico (dd/mm/aaaa).
5. **SECCIÓN DE RESPUESTA**	Apartados 1 a 5: selecciónense las casillas adecuadas. Apartado 2: si está en curso una HSE, es recomendable comunicar al solicitante el tiempo de tramitación (si se conoce). Apartado 6: a) Aunque la validación difiera de un país a otro o incluso entre instalaciones, se recomienda indicar la fecha de caducidad de la HSE. b) En los casos en que la fecha de caducidad de la garantía de la HSE sea indefinida, puede suprimirse este apartado. c) En cumplimiento de las disposiciones legales y reglamentarias nacionales pertinentes, corresponde al solicitante, o bien al contratista o subcontratista, solicitar la renovación de la HSE.
6. **OBSERVACIONES**	Información adicional con respecto a la HSE, la instalación o los aspectos anteriores.
7. **ANS O ASD EMISORA**	Indíquense el nombre de la autoridad emisora (en nombre de la ANS o ASD) y la fecha de la respuesta en formato numérico (dd/mm/aaaa).

FICHA DE INFORMACIÓN SOBRE LA HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO

(MODELO)

Deben cumplimentarse todas las casillas y el formulario debe presentarse a través de canales intergubernamentales o canales entre el Gobierno y la organización internacional.

SOLICITUD DE GARANTÍA DE LA HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO

A: _____

(nombre del país de la ANS o ASD)

Cumpliméntense los recuadros de respuesta, según proceda:

[] Proporciónese una garantía de la HSE de grado: [] S-UE/EU-S [] C-UE/EU-C

para las instalaciones que se enumeran a continuación

[] Incluida la protección de material o información clasificados

[] Incluidos los sistemas de información y comunicaciones («SIC») para el tratamiento de información clasificada

[] Iníciese, directamente o a petición de un contratista o subcontratista, el proceso de obtención de una HSE de grado ..... con grado de protección ..... y grado de SIC ....., si la instalación no posee actualmente estos grados.

Confírmese la exactitud de los datos de la instalación que figura a continuación y realícense las correcciones y añadidos necesarios.

1. Nombre completo de la instalación:	Correcciones y añadidos:
.....	.....
2. Dirección completa de la instalación:	
.....	.....
3. Dirección postal (si difiere del apartado 2)	
.....	.....
4. Código postal/localidad/país	
.....	.....
5. Nombre y apellidos del responsable de seguridad	
.....	.....
6. Teléfono/Fax/Correo electrónico del responsable de seguridad	
.....	.....

7. La presente solicitud se presenta por los siguientes motivos: [proporciónense datos de la fase precontractual (selección de propuestas), el contrato o subcontrato, el programa o el proyecto, etc.]

.....

ANS/ASD u órgano de contratación de la Comisión solicitante: Nombre: ..... Fecha: (dd.mm.yyyy) .....

RESPUESTA (en un plazo de diez días laborables)

Por la presente se certifica lo siguiente.

1. [] La instalación mencionada cuenta con una HSE de grado [] S-UE/EU-S

   [] C-UE/EU-C.

2. La instalación mencionada puede proteger información o material clasificados:

   [] sí, de grado: ..... [] no.

3. La instalación mencionada ha acreditado o autorizado el SIC:

   [] sí, de grado: ..... [] no.

4. [] En relación con la solicitud mencionada, se ha puesto en marcha el proceso de la HSE. Se le informará cuando se conceda o deniegue la HSE.

5. [] La instalación mencionada no tiene una HSE.

6. Esta garantía de la HSE caduca el: ..... (*dd/mm/aaaa*), o lo que indique la ANS o la ASD. En caso de invalidación previa o de modificación de la información arriba indicada, se le informará al respecto.

7. Observaciones:

   .....

ANS o ASD emisora *Nombre:* ..... *Fecha (dd/mm/aaaa):* .....

<Espacio reservado para la referencia a la legislación aplicable en materia de datos personales y el enlace a la información obligatoria para el interesado, por ejemplo, cómo se aplica el artículo 13 del Reglamento general de protección de datos ([2]).>

([2]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

Apéndice E

Requisitos mínimos para la protección de la ICUE en formato electrónico de grado RESTREINT UE/EU RESTRICTED manejada en el SIC del contratista

Generalidades

1. El contratista debe asegurarse de que la protección de la información clasificada de grado RESTREINT UE/EU RESTRICTED cumpla los requisitos mínimos de seguridad establecidos en esta cláusula de seguridad y cualesquiera otros requisitos adicionales aconsejados por el órgano de contratación o, en su caso, por la autoridad nacional de seguridad («ANS») o la autoridad de seguridad designada («ASD»).

2. Corresponde al contratista aplicar los requisitos de seguridad indicados en el presente documento.

3. A los efectos del presente documento, un sistema de información y comunicaciones («SIC») abarca todo el equipo utilizado para manejar, almacenar y transmitir ICUE, incluidas estaciones de trabajo, impresoras, fotocopiadoras, máquinas de fax, servidores, sistemas de gestión de red, controladores de red y controladores de comunicaciones, ordenadores portátiles, tabletas, teléfonos inteligentes y dispositivos de almacenamiento portátiles, tales como memorias USB, CD, tarjetas SD, etc.

4. El equipo especial, como los productos criptológicos, debe estar protegido de conformidad con su procedimiento operativo de seguridad específico.

5. Los contratistas deben crear una estructura responsable de la gestión de la seguridad del SIC que maneje información clasificada de grado RESTREINT UE/EU RESTRICTED y designar a un responsable de seguridad de la instalación de que se trate.

6. No estará permitido el uso de soluciones informáticas (equipo, programas o servicios informáticos) que sean propiedad privada del personal del contratista para almacenar o tratar información clasificada de grado RESTREINT UE/EU RESTRICTED.

7. La acreditación del SIC del contratista que maneje información clasificada de grado RESTREINT UE/EU RESTRICTED debe ser aprobada por la autoridad de acreditación de seguridad («AAS») del Estado miembro de que se trate o delegada en el responsable de seguridad del contratista, de conformidad con lo permitido por las disposiciones legales y reglamentarias nacionales.

8. Solo la información clasificada de grado RESTREINT UE/EU RESTRICTED que esté cifrada con productos criptológicos aprobados puede manejarse, almacenarse o transmitirse (por medios alámbricos o inalámbricos) como cualquier otra información no clasificada afectada por el contrato. Estos productos criptológicos deben ser aprobados por la UE o por un Estado miembro.

9. Las instalaciones externas implicadas en obras de mantenimiento o reparación deben estar obligadas contractualmente a cumplir las disposiciones aplicables para el manejo de la información clasificada de grado RESTREINT UE/EU RESTRICTED, tal como se establece en el presente documento.

10. A petición del órgano de contratación o de la ANS, la ASD o la AAS pertinente, el contratista debe presentar pruebas del cumplimiento de la cláusula de seguridad del contrato. Si también se solicita una auditoría e inspección de los procesos e instalaciones del contratista para garantizar el cumplimiento de estos requisitos, el contratista permitirá a los representantes del órgano de contratación, la ANS, la ASD o la AAS, o a la autoridad de seguridad de la UE pertinente, la realización de dicha auditoría e inspección.

Seguridad física

11. Los espacios en los que se utilicen los SIC para visualizar, almacenar, tratar o transmitir información de grado RESTREINT UE/EU RESTRICTED o los espacios que alojen servidores, sistemas de gestión de red, controladores de red y controladores de comunicaciones para dichos SIC deben delimitarse como zonas separadas y controladas con un sistema adecuado de control del acceso. El acceso a estas zonas separadas y controladas debe restringirse a las personas que posean una autorización específica. Sin perjuicio de lo dispuesto en el apartado 8, el equipo descrito en el apartado 3 debe almacenarse en dichas zonas separadas y controladas.

12. Deben implantarse mecanismos o procedimientos de seguridad para regular la introducción o la conexión de soportes informáticos de almacenamiento portátiles (como memorias USB, dispositivos de gran capacidad o CD regrabables) a componentes del SIC.

Acceso al SIC

13. El acceso al SIC del contratista que maneje ICUE se concede sobre la base de una necesidad de conocer estricta y por medio de autorizaciones del personal.

14. Todos los SIC deben disponer de listas actualizadas de los usuarios autorizados. Todos los usuarios deben estar autentificados al comienzo de cada sesión de tratamiento.

15. Las contraseñas, que forman parte de la mayoría de las medidas de seguridad de identificación y autentificación, deben ser de al menos nueve caracteres y deben incluir caracteres numéricos y «especiales» (si lo permite el sistema), así como caracteres alfabéticos. Las contraseñas deben cambiarse al menos cada 180 días. Deben modificarse a la mayor brevedad si se han visto comprometidas o han acabado en conocimiento de una persona no autorizada, o si se sospecha que alguno de esos dos casos haya podido suceder.

16. Todos los SIC deben contar con controles de acceso interno para impedir que los usuarios no autorizados accedan a información clasificada de grado RESTREINT UE/EU RESTRICTED o la modifiquen, o modifiquen el sistema y los controles de seguridad. Los usuarios deben ser desconectados automáticamente del SIC si sus terminales han estado inactivos durante un período predeterminado, o bien el SIC debe activar un protector de pantalla protegido mediante contraseña después de 15 minutos de inactividad.

17. A cada usuario del SIC se le asigna una cuenta y una clave de usuario únicas. La cuenta de usuario debe bloquearse automáticamente tras cinco intentos de conexión incorrectos seguidos.

18. Todos los usuarios del SIC deben estar informados de sus responsabilidades y de los procedimientos que deben seguirse para proteger la información clasificada de grado RESTREINT UE/EU RESTRICTED en el SIC. Las responsabilidades y los procedimientos que deben seguirse deben figurar en documentos por escrito, y los usuarios deben declarar por escrito que los conocen.

19. Los procedimientos operativos de seguridad deben estar a disposición de los usuarios y administradores e incluir descripciones de las funciones de seguridad y la lista de tareas, las instrucciones y los planes correspondientes.

Registros, auditoría y respuesta ante incidentes

20. Todo acceso al SIC debe quedar registrado.

21. Deben registrarse los sucesos siguientes:

    a) todos los intentos de conexión, exitosos o no;

    b) los cierres de sesión (también por inactividad, cuando proceda);

    c) la creación, supresión o modificación de derechos y privilegios de acceso;

    d) la creación, supresión o modificación de contraseñas.

22. En relación con todos los sucesos mencionados anteriormente, debe comunicarse como mínimo la información siguiente:

    a) tipo de suceso;

    b) clave de usuario;

    c) fecha y hora;

    d) identificación del dispositivo.

23. Los registros deben ayudar al responsable de seguridad a analizar posibles incidentes de seguridad. También pueden utilizarse para contribuir a cualquier investigación legal en caso de incidentes de seguridad. Todos los registros de seguridad deben comprobarse periódicamente para detectar posibles incidentes de seguridad. Los registros deben estar protegidos de supresiones o modificaciones no autorizadas.

24. El contratista debe tener una estrategia de respuesta para hacer frente a los incidentes de seguridad. Los usuarios y administradores deben recibir instrucciones sobre cómo responder a los incidentes, cómo notificarlos y qué hacer en caso de emergencia.

25. Debe notificarse al órgano de contratación todo comprometimiento o sospecha de comprometimiento de información clasificada de grado RESTREINT UE/EU RESTRICTED. Dicha notificación debe contener una descripción de la información en cuestión y de las circunstancias del comprometimiento o sospecha de comprometimiento. Debe informarse a todos los usuarios del SIC sobre cómo notificar al responsable de seguridad cualquier incidente de seguridad real o presunto.

Interconexión y redes

26. Cuando el SIC de un contratista que maneja información clasificada de grado RESTREINT UE/EU RESTRICTED está interconectado con un SIC que no está acreditado, aumenta significativamente la amenaza tanto para la seguridad del SIC como para la información de grado RESTREINT UE/EU RESTRICTED que maneja ese SIC. Dicha interconexión abarca internet y otros SIC públicos o privados, como otros SIC que sean propiedad del contratista o subcontratista. En este caso, el contratista debe realizar una evaluación del riesgo para determinar qué requisitos de seguridad adicionales deben aplicarse en el proceso de acreditación de seguridad. El contratista remitirá al órgano de contratación y, cuando así lo exijan las disposiciones legales y reglamentarias nacionales, a la AAS competente una declaración de conformidad que certifique que el SIC del contratista y las interconexiones correspondientes han sido acreditados para el manejo de ICUE de grado RESTREINT UE/EU RESTRICTED.

27. Está prohibido el acceso a distancia a servicios de red local desde otros sistemas (por ejemplo, acceso a distancia a correos electrónicos o servicios de apoyo de sistemas a distancia) a menos que el órgano de contratación adopte y ejecute medidas especiales de seguridad, que estén aprobadas por la AAS competente cuando así lo exijan las disposiciones legales y reglamentarias nacionales.

Gestión de configuraciones

28. Debe elaborarse una configuración pormenorizada del equipo y programas informáticos, en los términos que disponga la documentación de acreditación o aprobación (incluidos los diagramas de sistemas y de red), que debe actualizarse periódicamente.

29. El responsable de seguridad del contratista debe efectuar controles de configuración del equipo y programas informáticos para garantizar que no se haya introducido ninguno no autorizado.

30. Los cambios en la configuración del SIC del contratista deben evaluarse en términos de sus implicaciones para la seguridad y deben ser aprobados por el responsable de seguridad y, cuando así lo exijan las disposiciones legales y reglamentarias nacionales, la AAS.

31. El sistema debe examinarse para detectar vulnerabilidades de seguridad al menos una vez al trimestre. Deben instalarse y mantenerse actualizados programas informáticos de detección de programas maliciosos. Si es posible, dichos programas informáticos deben contar con una aprobación nacional o internacional reconocida, o ser programas estándar ampliamente aceptados en el sector.

32. El contratista debe elaborar un plan de continuidad de la actividad. Deben establecerse procedimientos de copia de seguridad que traten los aspectos siguientes:

a) la frecuencia de las copias de seguridad;

b) los requisitos de almacenamiento *in situ* (receptáculos ignífugos) o fuera del emplazamiento;

c) el control del acceso autorizado a copias de seguridad.

Saneamiento y destrucción

33. En el caso de SIC o soportes de almacenamiento de datos que tengan, en cualquier momento, información clasificada de grado RESTREINT UE/EU RESTRICTED, debe realizarse el proceso de saneamiento siguiente en todo el sistema o en los soportes de almacenamiento antes de su eliminación:

a) las memorias rápidas (por ejemplo, memorias USB, tarjetas SD, unidades de estado sólido y discos duros híbridos) deben sobrescribirse al menos tres veces y luego verificarse para asegurarse de que el contenido original no pueda recuperarse, o deben borrarse por medio de un programa informático aprobado de borrado;

b) los soportes magnéticos (por ejemplo, discos duros) deben sobrescribirse o desmagnetizarse;

c) los soportes ópticos (por ejemplo, CD y DVD) deben triturarse o desintegrarse;

d) respecto de los demás medios de almacenamiento, debe consultarse al órgano de contratación o, en su caso, la ANS, la ASD o la AAS sobre los requisitos de seguridad que deben cumplirse.

34. La información clasificada de grado RESTREINT UE/EU RESTRICTED que esté en un soporte de almacenamiento debe sanearse antes de entregarse a una entidad que no esté autorizada a acceder a información clasificada de grado RESTREINT UE/EU RESTRICTED (por ejemplo, para trabajos de mantenimiento).

ANEXO IV

Habilitación de seguridad de establecimiento y habilitación personal de seguridad para contratistas que manejen información clasificada de grado RESTREINT UE/EU RESTRICTED, y ANS o ASD a las que deben notificarse los contratos clasificados de grado RESTREINT UE/EU RESTRICTED ([1])

Estado miembro	HSE		Notificación a la ANS o ASD de un contrato o subcontrato que afecte a información de grado R-UE/EU-R		HPS	
	SÍ	NO	SÍ	NO	SÍ	NO
Bélgica		X		X		X
Bulgaria		X		X		X
Chequia		X		X		X
Dinamarca	X		X		X	
Alemania		X		X		X
Estonia	X		X			X
Irlanda		X		X		X
Grecia	X			X	X	
España		X	X			X
Francia		X		X		X
Croacia		X	X			X
Italia		X	X			X
Chipre		X	X			X
Letonia		X		X		X

([1]) Estos requisitos nacionales para las HSE y las HPS y las notificaciones de contratos que afecten a información clasificada de grado RESTREINT UE/EU RESTRICTED no deben imponer obligaciones adicionales a otros Estados miembros o a contratistas que estén bajo su jurisdicción.
Nota: las notificaciones de contratos que incluyan información de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET son obligatorias.

Estado miembro	HSE		Notificación a la ANS o ASD de un contrato o subcontrato que afecte a información de grado R-UE/EU-R		HPS	
	SÍ	NO	SÍ	NO	SÍ	NO
Lituania	X		X			X
Luxemburgo	X		X		X	
Hungría		X		X		X
Malta		X		X		X
Países Bajos	X (solo para los contratos en materia de defensa)		X (solo para los contratos en materia de defensa)			X
Austria		X		X		X
Polonia		X		X		X
Portugal		X		X		X
Rumanía		X		X		X
Eslovenia	X		X			X
Eslovaquia	X		X			X
Finlandia		X		X		X
Suecia	X (solo para los contratos en materia de defensa)		X (solo para los contratos en materia de defensa)		X (solo para los contratos en materia de defensa)	
Reino Unido		X		X		X

ANEXO V

LISTA DE SERVICIOS DE LAS AUTORIDADES DE SEGURIDAD NACIONALES O LAS AUTORIDADES DE SEGURIDAD DESIGNADAS RESPONSABLES DE TRAMITAR LOS PROCEDIMIENTOS EN MATERIA DE SEGURIDAD INDUSTRIAL

BÉLGICA

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes/Karmelietenstraat 15
1000 Bruxelles/Brussel
Teléfono: +32 25014542 (Secretaría)
Fax +32 25014596
Correo electrónico: nvo-ans@diplobel.fed.be

BULGARIA

1. State Commission on Information Security-National Security Authority
   Ulitsa Kozloduy 4
   1202 Sofia
   Teléfono: +359 29835775
   Fax +359 29873750
   Correo electrónico: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   Ulitsa Dyakon Ignatiy 3
   1092 Sofia
   Teléfono: +359 29227002
   Fax +359 29885211
   Correo electrónico: office@iksbg.org

3. State Intelligence Agency (security service)
   Ulitsa Hajduska Polyana 12
   1612 Sofia
   Teléfono: +359 29813221
   Fax +359 29862706
   Correo electrónico: office@dar.bg

4. State Agency for Technical Operations (security service)
   Ulitsa Shesti Septemvri 29
   1000 Sofia
   Teléfono: +359 29824971
   Fax +359 29461339
   Correo electrónico: dato@dato.bg

   (Las autoridades competentes enumeradas anteriormente llevan a cabo las pesquisas para la concesión de HSE a las personas jurídicas que vayan a celebrar un contrato clasificado y de HPS a las personas físicas que ejecuten un contrato clasificado para satisfacer las necesidades de estas autoridades).

5. State Agency National Security (security service)
   Bulevard Cherni Vrah 45
   1407 Sofia
   Teléfono: +359 28147109
   Fax +359 29632188, +359 28147441
   Correo electrónico: dans@dans.bg

   (El servicio de seguridad mencionado antes lleva a cabo las pesquisas para la concesión de HSE y de HPS a las demás personas jurídicas y personas físicas del país que vayan a celebrar un contrato clasificado o ejecuten un contrato clasificado).

CHEQUIA

National Security Authority
Industrial Security Department
Apdo. de correos 49
150 06 Praha 56
Teléfono: +420 257283129
Correo electrónico: sbr@nbu.cz

DINAMARCA

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Teléfono: +45 33148888
Fax +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Teléfono: +45 33325566
Fax +45 33931320

ALEMANIA

1. Para asuntos relativos a la política de seguridad industrial, las HSE o los planes de transporte [salvo en el caso de productos criptológicos o CCI (*Controlled Cryptographic Item*)]:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division-ZB3
Villemombler Str. 76
53123 Bonn
Teléfono: +49 228996154028
Fax +49 228996152676
Correo electrónico: dsagermany-zb3@bmwi.bund.de (buzón electrónico funcional)

2. Para las solicitudes de visita estándar de empresas alemanas o a estas:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Teléfono: +49 228996152401
Fax +49 228996152603
Correo electrónico: zb2-international@bmwi.bund.de (buzón electrónico funcional)

3. Planes de transporte de material criptológico:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Teléfono: +49 2289995826052
Fax +49 228991095826052
Correo electrónico: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Teléfono: +372 6939211
Fax +372 6935001
Correo electrónico: nsa@fis.gov.ee

IRLANDA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Teléfono: +353 14082724
Correo electrónico: nsa@dfa.ie

GRECIA

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
Leoforos Mesogeion 227-231
15561 Holargos, Athina
Teléfono: +30 2106572022, +30 2106572178
Fax +30 2106527612
Correo electrónico: daa.industrial@hndgs.mil.gr

ESPAÑA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Argentona, 30
28023 Madrid
Madrid
ESPAÑA
Tel. +34 913725000
Fax +34 913725808
Correo electrónico: nsa-sp@areatec.com
En materia de habilitaciones personales de seguridad: asip@areatec.com
En materia de planes de transporte y visitas internacionales: sp-ivtco@areatec.com

FRANCIA

National Security Authority (NSA) (para la elaboración y ejecución de políticas en ámbitos distintos de la defensa)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Teléfono: +33 171758193
Fax +33 171758200
Correo electrónico: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (para ejecución en el ámbito de la defensa)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 Boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15
Teléfono: +33 988670421
Correo electrónico: Para formularios y SdV salientes: dga-ssdi.ai.fct@intradef.gouv.fr
Para SdV entrantes: dga-ssdi.visit.fct@intradef.gouv.fr

CROACIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Teléfono: +385 14681222
Fax +385 14686049
Correo electrónico: NSACroatia@uvns.hr

ITALIA

Presidenza del Consiglio dei Ministri
D.I.S.-U.C.Se.
Via di Santa Susanna 15
00187 Roma
Teléfono: +39 0661174266
Fax +39 064885273

CHIPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
Correo electrónico: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
Leoforos Strovolos 172-174
2048 Strovolos, Lefkosía
Teléfono: +357 22807569, +357 22807764
Fax +357 22302351
Correo electrónico: cynsa@mod.gov.cy

LETONIA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
Apdo. de correos 286
Riga LV-1001
Teléfono: +371 67025418, +371 67025463
Fax +371 67025454
Correo electrónico: ndi@sab.gov.lt, ndi@zd.gov.lv

LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Teléfono: +370 70666703, +370 70666701
Fax +370 70666700
Correo electrónico: nsa@vsd.lt

LUXEMBURGO

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Teléfono: +352 24782210
Correo electrónico: ans@me.etat.lu

HUNGRÍA

National Security Authority of Hungary
H-1399 Budapest; apdo. de correos 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Teléfono: +36 13911862
Fax +36 13911889
Correo electrónico: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Teléfono: +356 23952000
Fax +356 21242406
Correo electrónico: certification@mccaa.org.mt

PAÍSES BAJOS

1. Ministry of the Interior and Kingdom Relations
Apdo. de correos 20010
2500 EA Den Haag
Teléfono: +31 703204400
Fax +31 703200733
Correo electrónico: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
Apdo. de correos 20701
2500 ES Den Haag
Teléfono: +31 704419407
Fax +31 703459189
Correo electrónico: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Wien
Teléfono: +43 153115202594
Correo electrónico: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt
Postfach 2000
1030 Wien
Correo electrónico: abwa@bmlvs.gv.at

POLONIA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warszawa
Teléfono: +48 225857944
Fax +48 225857443
Correo electrónico: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira n.º 69
1300-342 Lisboa
Teléfono: +351 213031710
Fax +351 213031711
Correo electrónico: sind@gns.gov.pt, franco@gns.gov.pt

RUMANÍA

Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS)
Romanian NSA-ORNISS-National Registry Office for Classified Information
Strada Mureş 4
012275 Bucureşti
Teléfono: +40 212075115
Fax +40 212245830
Correo electrónico: relatii.publice@orniss.ro, nsa.romania@nsa.ro

ESLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Teléfono: +386 14781390
Fax +386 14781399
Correo electrónico: gp.uvtp@gov.si

ESLOVAQUIA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Teléfono: +421 268691111
Fax +421 268691700
Correo electrónico: podatelna@nbu.gov.sk

FINLANDIA

National Security Authority
Ministry for Foreign Affairs
Apdo. de correos 453
FI-00023 Gobierno
Correo electrónico: NSA@formin.fi

SUECIA

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Teléfono: +46 84051000
   Fax +46 87231176
   Correo electrónico: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Teléfono: +46 87824000
   Fax +46 87826900
   Correo electrónico: security@fmv.se

REINO UNIDO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Teléfono: +44 2072765497, +44 2072765645
Correo electrónico: UK-NSA@cabinet-office.x.gsi.gov.uk