DECISIÓN (UE, EURATOM) 2021/259 DE LA COMISIÓN

de 10 de febrero de 2021

por la que se establecen normas de desarrollo sobre la seguridad industrial en relación con las subvenciones clasificadas

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,

Visto el 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 se deroga el Reglamento (UE, Euratom) n.º 966/2012 ([1]),

Vista la Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión ([2]),

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 ([3]),

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 ([4]),

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 de la Comisión,

Considerando lo siguiente:

(1) Los artículos 41, 42, 47 y 48 de la Decisión (UE, Euratom) 2015/444 establecen que, a fin de completar y facilitar la aplicación del capítulo 6 de dicha Decisión, deben adoptarse normas de desarrollo sobre seguridad industrial que contengan disposiciones más pormenorizadas acerca de cuestiones como la adjudicación de acuerdos de subvención 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 acuerdos de subvención 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 de que se trate. 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 (2011/C 202/05) ([5]).

([1]) DO L 193 de 30.7.2018, p. 1.
([2]) DO L 72 de 17.3.2015, p. 41.
([3]) DO L 72 de 17.3.2015, p. 53.
([4]) DO L 6 de 11.1.2017, p. 40.
([5]) DO C 202 de 8.7.2011, p. 13.

(3) El Consejo, la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad han acordado asegurar una coherencia máxima en la aplicación de las normas de seguridad relativas a la 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 ([6]) del Consejo, relativa a 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 las subvenciones clasificadas 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.

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

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 las subvenciones clasificadas en el sentido 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) en la publicación de convocatorias, en la concesión de subvenciones y en la ejecución de los acuerdos de subvención clasificados celebrados por la Comisión Europea.

3. La presente Decisión se refiere a las subvenciones que implican información clasificada de los grados siguientes:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

4. La presente Decisión se aplicará sin perjuicio de las normas específicas establecidas en otros actos jurídicos, como las relativas al Programa Europeo de Desarrollo Industrial en materia de Defensa.

Artículo 2

Responsabilidades dentro de la Comisión

1. Como parte de las responsabilidades del ordenador de la autoridad que concede la subvención a que se refiere el Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, dicha persona se asegurará de que la subvención clasificada cumpla lo dispuesto en la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo.

([6]) 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).

([7]) Decisión de la Comisión, de 4 de mayo de 2016, sobre la capacitación en materia de seguridad [C(2016) 2797 final].

2. A tal fin, el ordenador competente solicitará, en todas las fases, el dictamen de la autoridad de seguridad de la Comisión sobre las cuestiones relativas a los elementos de seguridad de un acuerdo de subvención, programa o proyecto clasificados, e informará al responsable local de seguridad acerca de los acuerdos de subvención clasificados que se hayan firmado. La decisión sobre el grado de clasificación de temas específicos corresponderá a la autoridad que concede la subvención y se tomará teniendo debidamente en cuenta la guía de clasificación de seguridad.

3. Cuando se apliquen las instrucciones de seguridad del programa o proyecto a que se refiere el artículo 5, apartado 3, la autoridad que concede la subvención y la autoridad de seguridad de la Comisión desempeñarán las responsabilidades que se les asignan en dichas instrucciones.

4. 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.

5. Cuando las subvenciones sean gestionadas por agencias ejecutivas u otros organismos de financiación de la UE y no se apliquen las normas específicas establecidas en otros actos jurídicos mencionados en el artículo 1, apartado 4:

a) el servicio delegante de la Comisión ejercerá los derechos relativos al originador de la ICUE generada en el contexto de las subvenciones, si así lo disponen los acuerdos de delegación;

b) el servicio delegante de la Comisión se encargará de determinar la clasificación de seguridad;

c) las solicitudes de información sobre la habilitación de seguridad y las notificaciones a las ANS o ASD se enviarán a través de la autoridad de seguridad de la Comisión.

CAPÍTULO 2

TRAMITACIÓN DE CONVOCATORIAS DE SUBVENCIONES CLASIFICADAS

Artículo 3

Principios básicos

1. Las partes clasificadas de las subvenciones serán ejecutadas únicamente por beneficiarios registrados en un Estado miembro o por beneficiarios 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 o suscrito un acuerdo administrativo con la Comisión ([8]).

2. Antes de publicar la convocatoria de una subvención clasificada, la autoridad que concede la subvención determinará la clasificación de seguridad de toda la información que pueda proporcionarse a los solicitantes. La autoridad que concede la subvención determinará asimismo la clasificación de seguridad máxima de la información que pueda utilizarse o generarse durante la ejecución del acuerdo de subvención, 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) clasificado.

3. La autoridad que concede la subvención se asegurará de que las convocatorias de subvenciones clasificadas proporcionen información sobre las obligaciones especiales en materia de seguridad relacionadas con la información clasificada. La documentación de la convocatoria incluirá aclaraciones sobre el calendario para que los beneficiarios obtengan las HSE, en caso necesario. Los anexos I y II contienen ejemplos de modelos para la información relativa a las condiciones de las convocatorias.

([8]) 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.

4. La autoridad que concede la subvención 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 solicitantes 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, sus normas de desarrollo y la legislación nacional aplicable.

5. Cuando se proporcione información de grado RESTREINT UE/EU RESTRICTED a los solicitantes, los requisitos mínimos mencionados en el artículo 5, apartado 7, de la presente Decisión se incluirán en la convocatoria o en los acuerdos de confidencialidad celebrados durante la fase de propuesta.

6. Todos los solicitantes y beneficiarios que deban manejar o almacenar información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET en sus instalaciones, ya sea en la fase de propuesta o durante la ejecución del propio acuerdo de subvención clasificado, dispondrán de una HSE del grado requerido, excepto en los casos mencionados en el apartado 9. A continuación, se especifican los tres supuestos que pueden darse durante la fase de propuesta de una subvención clasificada 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 propuesta:

   cuando la convocatoria se refiera a una subvención que incluirá ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, pero no requiera que el solicitante maneje dicha información en la fase de propuesta, el solicitante que no disponga de una HSE del grado exigido no será excluido 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 de la autoridad que concede la subvención durante la fase de propuesta:

   se concederá acceso al personal del solicitante que esté en posesión de una HPS del grado exigido y que tenga necesidad de conocer la información.

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

   cuando la convocatoria requiera que los solicitantes manejen o almacenen ICUE en sus locales, el solicitante deberá disponer de una HSE del grado exigido. En tales circunstancias, la autoridad que concede la subvención obtendrá, a través de la autoridad de seguridad de la Comisión, una garantía de la ANS o ASD correspondiente de que al solicitante se le ha concedido una HSE adecuada antes de que se le facilite material con ICUE. Se concederá acceso al personal del solicitante que esté en posesión de una HPS del grado exigido y que tenga necesidad de conocer la información.

7. En principio, no se exigirá una HSE o una HPS para acceder a información de grado RESTREINT UE/EU RESTRICTED, ya sea en la fase de propuesta o para la ejecución del acuerdo de subvención. Cuando los Estados miembros exijan una HSE o una HPS para los acuerdos de subvención 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 solicitantes, beneficiarios o subcontratistas de los Estados miembros que no dispongan de tales requisitos de HSE o HPS para el acceso a información de grado RESTREINT UE/EU RESTRICTED de los acuerdos de subvención o subcontratos correspondientes o de competir para que se les adjudiquen. Dichos acuerdos de subvención se ejecutarán en los Estados miembros de conformidad con sus disposiciones legales y reglamentarias nacionales.

8. Cuando se requiera una HSE para la tramitación de una convocatoria y para la ejecución de un acuerdo de subvención clasificado, la autoridad que concede la subvención presentará, a través de la autoridad de seguridad de la Comisión, una solicitud a la ANS o ASD del beneficiario utilizando una ficha de información sobre la habilitación de seguridad de establecimiento o cualquier formulario electrónico equivalente establecido. El anexo III, apéndice D, contiene un ejemplo de ficha de información sobre la habilitación de seguridad de establecimiento ([9]). La respuesta a una ficha de información sobre la habilitación de seguridad de establecimiento se proporcionará, en la medida de lo posible, en un plazo de diez días laborables a partir de la fecha de la solicitud.

9. Cuando los establecimientos gubernamentales de los Estados miembros o los establecimientos bajo su control oficial participen en subvenciones clasificadas que requieran HSE, y cuando no se expidan HSE para dichos establecimientos con arreglo a la legislación nacional, la autoridad que concede la subvención comprobará con la ANS o la ASD de que se trate, a través de la autoridad de seguridad de la Comisión, si dichos establecimientos gubernamentales son capaces de manejar ICUE del grado requerido.

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

10. Cuando se requiera una HPS para la ejecución de un acuerdo de subvención clasificado y cuando, con arreglo a las normas nacionales, sea necesaria una HSE antes de conceder una HPS, la autoridad que concede la subvención comprobará con la ANS o ASD del beneficiario, a través de la autoridad de seguridad de la Comisión, utilizando una ficha de información sobre la habilitación de seguridad de establecimiento, que el beneficiario disponga de una HSE o que el proceso de la HSE esté en curso. En este caso, la Comisión no expedirá solicitudes de HPS utilizando la ficha de información sobre la habilitación personal de seguridad.

Artículo 4

Subcontratación en el marco de subvenciones clasificadas

1. Las condiciones en las que los beneficiarios podrán subcontratar tareas que impliquen ICUE se definirán en la convocatoria y en el acuerdo de subvención. Estas condiciones incluirán el requisito de que todas las fichas de información sobre la habilitación de seguridad de establecimiento se presenten a través de la autoridad de seguridad de la Comisión. La subcontratación estará supeditada al consentimiento previo por escrito de la autoridad que concede la subvención. En su caso, la subcontratación se ajustará al acto de base por el que se establezca el programa.

2. Las partes clasificadas de las subvenciones serán subcontratadas únicamente a entidades registradas en un Estado miembro o a entidades registradas en un tercer país o creadas por una organización internacional cuando dicho tercer país u organización internacional haya celebrado un acuerdo sobre seguridad de la información con la Unión o suscrito un acuerdo administrativo con la Comisión ([10]).

CAPÍTULO 3

TRAMITACIÓN DE LAS SUBVENCIONES CLASIFICADAS

Artículo 5

Principios básicos

1. Al adjudicar una subvención clasificada, la autoridad que concede la subvención, junto con la autoridad de seguridad de la Comisión, se asegurará de que las obligaciones del beneficiario relativas a la protección de la ICUE utilizada o generada durante la ejecución del acuerdo de subvención formen parte de dicho acuerdo. Los requisitos de seguridad específicos de la subvención se describirán en la cláusula sobre aspectos de la seguridad. En el anexo III figura un ejemplo de modelo de cláusula sobre aspectos de la seguridad.

2. Antes de firmar una subvención clasificada, la autoridad que concede la subvención aprobará una guía de clasificación de seguridad en relación con las tareas que deberán realizarse y la información generada durante la ejecución de la subvención o, en su caso, a nivel de programa o proyecto. La cláusula sobre aspectos de la seguridad incluirá la guía de clasificación de seguridad.

3. Los requisitos de seguridad específicos del programa o proyecto se describirán en las instrucciones de seguridad del programa (o proyecto). Las instrucciones de seguridad de un programa o proyecto podrán redactarse utilizando las disposiciones del modelo de la cláusula sobre aspectos de la seguridad 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 acuerdo de subvención sea parte de un programa o proyecto que tenga sus propias instrucciones de seguridad de programa o proyecto, la cláusula sobre aspectos de la seguridad del acuerdo de subvención adoptará una forma simplificada e incluirá una referencia a las disposiciones en materia de seguridad establecidas en las instrucciones de seguridad del programa o proyecto.

4. Excepto en los casos mencionados en el artículo 3, apartado 9, el acuerdo de subvención clasificado no se firmará hasta que la ANS o ASD del solicitante haya confirmado la HSE del solicitante o, cuando el acuerdo de subvención clasificado se adjudique a un consorcio, hasta que la ANS o ASD de al menos un solicitante, dentro del consorcio, o, en caso necesario, de más de un solicitante, haya confirmado la HSE del solicitante.

5. En principio, y salvo disposición en contrario en otras normas pertinentes, la autoridad que concede la subvención será considerada la originadora de la ICUE generada en la ejecución del acuerdo de subvención.

([10]) 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.

6. La autoridad que concede la subvención notificará, a través de la autoridad de seguridad de la Comisión, a las ANS y/o ASD de todos los beneficiarios y subcontratistas la firma de acuerdos de subvención o subcontratos clasificados y los casos de extinción anticipada o las prórrogas de dichos acuerdos o subcontratos. En el anexo IV figura una lista de requisitos por países.

7. Los acuerdos de subvención que incluyan información clasificada de grado RESTREINT UE/EU RESTRICTED contendrán una cláusula de seguridad que haga vinculantes para los beneficiarios las disposiciones del anexo III, apéndice E. Estos acuerdos de subvención incluirán una cláusula sobre aspectos de la seguridad 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 beneficiario para la acreditación del SIC del beneficiario que maneje la información de grado RESTREINT UE/EU RESTRICTED.

8. Cuando así lo exijan las disposiciones legales y reglamentarias de los Estados miembros, las ANS o ASD se asegurarán de que los beneficiarios 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 realizarán visitas de verificación a las instalaciones de los beneficiarios o subcontratistas situadas en su territorio. Cuando la ANS o la ASD no esté sujeta a dicha obligación, la autoridad que concede la subvención se asegurará de que los beneficiarios apliquen las disposiciones de seguridad exigidas según lo dispuesto en el anexo III, apéndice E.

Artículo 6

Acceso del personal de los beneficiarios y subcontratistas a ICUE

1. La autoridad que concede la subvención se asegurará de que los acuerdos de subvención clasificados contengan disposiciones que establezcan que al personal del beneficiario o subcontratista que necesite acceder a la ICUE para la ejecución del acuerdo de subvención o subcontrato clasificado solo se le concederá dicho acceso si:

a) se ha corroborado que tiene necesidad de conocer la información;

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

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. Cuando proceda, el acceso a la ICUE también se ajustará al acto de base por el que se establezca el programa y tendrá en cuenta cualquier marca adicional definida en la guía de clasificación de seguridad.

3. Si un beneficiario 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 beneficiario 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.

Artículo 7

Acceso a la ICUE por expertos que participan en controles, revisiones o auditorías

1. Cuando en controles, revisiones o auditorías llevadas a cabo por la autoridad que concede la subvención o en revisiones de rendimiento de los beneficiarios que requieran acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET participen personas externas («expertos»), solo se proporcionará un contrato a estas personas si han obtenido una habilitación de seguridad del grado pertinente expedido por la ANS o ASD respectiva o cualquier otra autoridad de seguridad competente. La autoridad que concede la subvención, a través de la autoridad de seguridad de la Comisión, comprobará y, en caso necesario, pedirá a la ANS o ASD que inicie el proceso de verificación de expertos al menos seis meses antes del inicio de sus respectivos contratos.

2. Antes de la firma de sus contratos, los expertos serán instruidos sobre las normas de seguridad aplicables para la protección de la ICUE y habrán aceptado sus responsabilidades en lo que respecta a la protección de dicha información.

CAPÍTULO 4

VISITAS EN RELACIÓN CON ACUERDOS DE SUBVENCIÓN CLASIFICADOS

Artículo 8

Principios básicos

1. Cuando la autoridad que concede la subvención, los expertos, los beneficiarios 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 en el contexto de la ejecución de un acuerdo de subvención clasificado, se organizarán visitas, con la colaboración de las ANS, las ASD o cualesquiera otras autoridades de seguridad competentes.

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 la subvención clasificada;

b) todos los visitantes deberán estar en posesión de una HPS del grado exigido y tener necesidad de conocer la información para acceder a la ICUE utilizada o generada durante la ejecución de una subvención clasificada.

Artículo 9

Solicitudes de visita

1. Las visitas de los beneficiarios o subcontratistas a las instalaciones de otros beneficiarios o subcontratistas o a los locales de la autoridad que concede la subvención 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 deberá confirmar la HPS del visitante antes de presentar la *SdV* a la ANS o ASD de la instalación que lo recibe (o la autoridad de seguridad de la Comisión si la visita se realiza en los locales de una autoridad que concede la subvención).

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, expertos o auditores de la autoridad que concede la subvención a las instalaciones de los beneficiarios o subcontratistas 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 visita 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* deberán presentarse a la autoridad de seguridad competente de la instalación que recibe la visita al menos quince días laborables antes de la fecha de esta.

Artículo 10

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, en el que figurarán 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 11

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 en relación con una subvención clasificada específica 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 instrucciones de seguridad de un programa o proyecto o en otros acuerdos específicos. En estos supuestos, no serán de aplicación los procedimientos establecidos en el artículo 9 y el artículo 10, 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 9 y el artículo 10, apartado 1.

CAPÍTULO 5

TRANSMISIÓN Y TRANSPORTE DE ICUE PARA LA EJECUCIÓN DE ACUERDOS DE SUBVENCIÓN CLASIFICADOS

Artículo 12

Principios básicos

La autoridad que concede la subvención 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 acuerdo de subvención clasificado, incluido el consentimiento del originador.

Artículo 13

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.

El sistema de información y comunicaciones que sea propiedad de un beneficiario y se utilice para manejar la ICUE necesaria para la ejecución del acuerdo de subvención (SIC del beneficiario) tendrá que ser acreditado 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 de seguridad TEMPEST se ejecutarán de conformidad con el artículo 36, apartado 6, de dicha Decisión.

2. La acreditación de seguridad del SIC del beneficiario que maneje ICUE de grado RESTREINT UE/EU RESTRICTED y cualquier interconexión de este podrán delegarse en el responsable de seguridad del beneficiario si así lo permiten las disposiciones legales y reglamentarias nacionales. Cuando esta tarea sea delegada, el beneficiario será responsable de respetar los requisitos mínimos de seguridad descritos en la cláusula sobre aspectos de la seguridad al manejar información de grado RESTREINT UE/EU RESTRICTED en su SIC. Sin embargo, las ANS, las ASD y las AAS pertinentes seguirán siendo responsables de la protección de la información de grado RESTREINT UE/EU RESTRICTED que manejen los beneficiarios y seguirán gozando de la facultad de examinar las medidas de seguridad adoptadas por los beneficiarios. Además, el beneficiario remitirá a la autoridad que concede la subvención, 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 beneficiario y las interconexiones correspondientes han sido acreditados para el manejo de la ICUE de grado RESTREINT UE/EU RESTRICTED ([11]).

Artículo 14

Transporte por medio de correo comercial

El transporte de la ICUE por correo comercial se ajustará a las disposiciones pertinentes de la Decisión (UE, Euratom) 2019/1962 de la Comisión ([12]), por la que se establecen las normas de desarrollo aplicables al manejo de la información RESTREINT UE/EU RESTRICTED, y de la Decisión (UE, Euratom) 2019/1961 de la Comisión ([13]), por la que se establecen las normas de desarrollo aplicables al manejo de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET.

Artículo 15

Transporte en mano

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

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

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

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 la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, el transporte en mano por parte del personal del beneficiario dentro de un Estado miembro 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 permitirá 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.

([11]) 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.

([12]) Decisión (UE, Euratom) 2019/1962 de la Comisión, de 17 de octubre de 2019, por la que se establecen las normas de desarrollo aplicables al manejo de la información RESTREINT UE/EU RESTRICTED (DO L 311 de 2.12.2019, p. 21).

([13]) Decisión (UE, Euratom) 2019/1961 de la Comisión, de 17 de octubre de 2019, por la que se establecen las normas de desarrollo aplicables al manejo de la información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET (DO L 311 de 2.12.2019, p. 1).

4. Para el transporte en mano de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET de un Estado miembro a otro por parte del personal del beneficiario, 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 será informado de todas las obligaciones en materia de seguridad que deban observarse durante el transporte y firmará una declaración de conocimiento 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) deberá 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 beneficiario 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 o la Comisión y dicho tercer país u organización internacional.

CAPÍTULO 6

PLAN DE CONTINUIDAD DE LA ACTIVIDAD

Artículo 16

Planes de contingencia y medidas de recuperación

La autoridad que concede la subvención se asegurará de que el acuerdo de subvención clasificado obligue al beneficiario a establecer planes de contingencia empresarial para proteger, en situaciones de emergencia, la ICUE manejada en el contexto de la subvención clasificada, 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. Los beneficiarios confirmarán a la autoridad que concede la subvención la existencia de sus planes de contingencia empresarial.

Artículo 17

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 10 de febrero de 2021.

Por la Comisión,
en nombre de la Presidenta,
Johannes HAHN
Miembro de la Comisión

ANEXO I

INFORMACIÓN ESTÁNDAR EN LA CONVOCATORIA

(adaptar a la convocatoria utilizada)

Seguridad

Los proyectos que impliquen información clasificada de la UE deberán someterse a un control de seguridad para autorizar la financiación y podrán estar sujetos a normas de seguridad específicas (detalladas en una cláusula sobre aspectos de la seguridad adjunta al acuerdo de subvención).

Estas normas [regidas por la Decisión (UE, Euratom) 2015/444 de la Comisión ([1]) y/o las normas nacionales] establecen, por ejemplo, lo siguiente:

— Los proyectos que contengan información clasificada de grado TRES SECRET UE/EU TOP SECRET (o equivalente) **NO** podrán financiarse.

— La información clasificada deberá marcarse de acuerdo con las instrucciones de seguridad aplicables que figuren en la cláusula sobre aspectos de la seguridad.

— La información con el grado de clasificación CONFIDENTIEL UE/EU CONFIDENTIAL o un grado superior (y RESTREINT UE/EU RESTRICTED si así lo exigen las normas nacionales) podrá ser:

  — creada o consultada solo en locales con habilitación de seguridad de establecimiento por parte de la Autoridad Nacional de Seguridad (ANS) competente, de conformidad con las normas nacionales,

  — manejada únicamente en una zona segura acreditada por la ANS competente,

  — generada y manejada solo por personas con una habilitación personal de seguridad (HPS) válida y que tengan la necesidad de conocer la información.

— Al final de la subvención, la información clasificada deberá devolverse o seguir estando protegida de conformidad con las normas aplicables.

— Las tareas encomendadas que impliquen información clasificada de la UE (ICUE) solo podrán subcontratarse previa aprobación por escrito de la autoridad que concede la subvención y únicamente a entidades establecidas en un Estado miembro de la UE o en un país no perteneciente a la UE que haya celebrado un acuerdo de seguridad de la información con la UE (o un acuerdo administrativo con la Comisión).

— La revelación de la ICUE a terceros estará sujeta a la aprobación previa por escrito de la autoridad que concede la subvención.

Téngase en cuenta que, dependiendo del tipo de actividad, podrá ser necesario facilitar la habilitación de seguridad de establecimiento antes de la firma de la subvención. La autoridad que concede la subvención evaluará la necesidad de habilitaciones en cada caso y fijará su fecha de entrega durante la preparación de la subvención. Téngase en cuenta que **en ningún caso** podremos firmar ningún acuerdo de subvención hasta que al menos uno de los beneficiarios de un consorcio disponga de una habilitación de seguridad de establecimiento.

Podrán añadirse otras recomendaciones de seguridad al acuerdo de subvención en forma de prestaciones de seguridad (*por ejemplo, crear un grupo consultivo de seguridad, limitar el nivel de detalle, utilizar un supuesto falso, excluir el uso de información clasificada, etc.*).

Los beneficiarios deberán garantizar que sus proyectos no estén sujetos a requisitos de seguridad nacionales o de terceros países que puedan afectar a la ejecución o poner en tela de juicio la concesión de la subvención (*por ejemplo, restricciones tecnológicas, clasificación de seguridad nacional, etc.*). La autoridad que concede la subvención deberá ser informada inmediatamente de cualquier posible problema en relación con la seguridad.

[OPCIÓN adicional para los acuerdos marco de colaboración: En el caso de los acuerdos marco de colaboración, tanto las solicitudes de cooperación marco como las solicitudes de subvención pueden tener que someterse a un examen de seguridad.]

([1]) Véase la Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

ANEXO II

CLÁUSULAS DEL MODELO DEL ACUERDO DE SUBVENCIÓN

(adaptar al acuerdo de subvención utilizado)

13.2 Seguridad: información clasificada

Las partes deberán manejar la información clasificada (de la UE o nacional) de conformidad con la legislación de la UE o nacional aplicable en materia de información clasificada [en particular, la Decisión (UE, Euratom) 2015/444 de la Comisión ([1]) y sus normas de desarrollo].

En el anexo 5 se establecen normas de seguridad específicas (si las hubiere).

ANEXO 5

Seguridad: información clasificada de la UE

[OPCIÓN para las acciones con información clasificada de la UE (estándar): Si la información clasificada de la UE es utilizada o generada por la acción, dicha información deberá tratarse de acuerdo con la cláusula sobre aspectos de la seguridad y su guía de clasificación de seguridad, que figuran en el anexo 1, y la Decisión (UE, Euratom) 2015/444 y sus normas de desarrollo, hasta que se desclasifique.

Los entregables que contengan información clasificada de la UE deberán enviarse con arreglo a los procedimientos especiales acordados con la autoridad que concede la subvención.

Las tareas encomendadas que impliquen información clasificada de la UE (ICUE) solo podrán subcontratarse previa aprobación explícita por escrito de la autoridad que concede la subvención y únicamente a entidades establecidas en un Estado miembro de la UE o en un país no perteneciente a la UE que haya celebrado un acuerdo de seguridad de la información con la UE (o un acuerdo administrativo con la Comisión).

La información clasificada de la UE no podrá revelarse a ningún tercero (incluidos los participantes en la ejecución de la acción) sin la aprobación previa, expresa y por escrito, de la autoridad que concede la subvención.]

([1]) 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).

ANEXO III

[Anexo IV (de.....)]

CLÁUSULA SOBRE ASPECTOS DE LA SEGURIDAD [1]

[Modelo]

[1] El presente modelo de cláusula sobre aspectos de la seguridad se aplicará cuando la Comisión se considere la originadora de información clasificada creada y tratada a efectos de la ejecución del acuerdo de subvención. Cuando el originador de la información clasificada generada y manejada para la ejecución del acuerdo de subvención no sea la Comisión, y cuando los Estados miembros que participen en la subvención establezcan un marco de seguridad específico, podrán aplicarse otros modelos de cláusula sobre aspectos de la seguridad.

Apéndice A

REQUISITOS DE SEGURIDAD

La autoridad que concede la subvención deberá incluir los siguientes requisitos de seguridad en la cláusula sobre aspectos de la seguridad. Es posible que algunas cláusulas no se apliquen al acuerdo de subvención. Tales cláusulas se muestran entre corchetes.

La lista de cláusulas no es exhaustiva. Podrán añadirse cláusulas adicionales dependiendo de la naturaleza de la subvención clasificada.

CONDICIONES GENERALES [*N.B.: Aplicable a todos los acuerdos de subvención clasificados*]

1. La presente cláusula sobre aspectos de la seguridad forma parte del acuerdo de subvención [o subcontrato] clasificado y describe los requisitos de seguridad específicos del acuerdo de subvención. El incumplimiento de estos requisitos podrá ser motivo suficiente para que la rescisión del acuerdo de subvención.

2. Los beneficiarios de subvenciones están sujetos a todas las obligaciones establecidas en la Decisión (UE, Euratom) 2015/444 ([2]) de la Comisión (en lo sucesivo «DC 2015/444») y sus normas de desarrollo ([3]). Si el beneficiario de la subvención se enfrenta a un problema de aplicación del marco jurídico aplicable en un Estado miembro, deberá dirigirse a la autoridad de seguridad de la Comisión y a la Autoridad Nacional de Seguridad (ANS) o a la Autoridad de Seguridad Designada (ASD).

3. La información clasificada generada durante la ejecución del acuerdo de subvención deberá 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 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 guía de clasificación de seguridad si media la autorización escrita de la autoridad que concede la subvención.

4. En su calidad de autoridad que concede la subvención, la Comisión ejercerá los derechos del originador de toda ICUE producida y manejada para la ejecución del acuerdo de subvención clasificado.

5. Sin el consentimiento por escrito de la autoridad que concede la subvención, el beneficiario o subcontratista no podrá utilizar la información o el material proporcionados por la autoridad que concede la subvención o generados en su nombre para ningún fin distinto del previsto en el acuerdo de subvención.

6. Cuando se requiera una habilitación de seguridad de establecimiento (HSE) para la ejecución de un acuerdo de subvención, el beneficiario deberá pedir a la autoridad que concede la subvención que tramite la solicitud de dicha habilitación.

7. El beneficiario deberá investigar todos los fallos de seguridad relacionados con la ICUE y notificarlos a la autoridad que concede la subvención tan pronto como sea posible. El beneficiario o subcontratista deberá 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 acuerdo de subvención se ha perdido o ha acabado en conocimiento de personas no autorizadas.

([2]) 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).

([3]) La autoridad que concede la subvención deberá introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

8. Al concluir el acuerdo de subvención, el beneficiario o subcontratista devolverá toda ICUE que obre en su poder a la autoridad que concede la subvención con la mayor brevedad posible. Cuando sea viable, el beneficiario o subcontratista podrá destruir la ICUE en lugar de devolverla. Esto se hará con arreglo a las disposiciones legales y reglamentarias del país en que esté establecido el beneficiario, previo consentimiento y siguiendo las instrucciones de la autoridad de seguridad de la Comisión. La ICUE se destruirá de tal forma que no pueda reconstruirse, ya sea en todo o en parte.

9. Cuando el beneficiario o subcontratista esté autorizado a conservar la ICUE tras resolverse o finalizar el acuerdo de subvención, debe seguir estando protegida de conformidad con la DC 2015/444 y sus normas de desarrollo ([4]).

10. Todo manejo, tratamiento y transmisión electrónicos de la ICUE deberá 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 se acrediten los sistemas de información y comunicaciones que sean de propiedad del beneficiario y se utilicen para manejar la ICUE a efectos del acuerdo de subvención («SIC del beneficiario») ([5]); 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 de seguridad TEMPEST de conformidad con el artículo 36, apartado 6, de la DC 2015/444.

11. El beneficiario o subcontratista deberá contar con planes de contingencia empresarial para proteger, en situaciones de emergencia, toda ICUE manejada durante la ejecución del acuerdo de subvención clasificado y deberá adoptar medidas preventivas y de recuperación para minimizar el efecto de los incidentes relacionados con el manejo y el almacenamiento de la ICUE. El beneficiario o subcontratista deberá informar a la autoridad que concede la subvención de su plan de contingencia.

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

12. En principio, no es necesario estar en posesión de una habilitación personal de seguridad (HPS) para el cumplimiento del acuerdo de subvención ([6]). No obstante, solo podrá acceder a la información o el material clasificado de grado RESTREINT UE/EU RESTRICTED el personal del beneficiario que necesite dicha información para ejecutar el acuerdo de subvención (principio de necesidad de conocer la información), que haya sido informado por el responsable de seguridad del beneficiario 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.

13. Salvo que la autoridad que concede la subvención dé su consentimiento por escrito, el beneficiario o subcontratista no podrá 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 la información.

14. El beneficiario o subcontratista deberá mantener las marcas de clasificación de seguridad de la información clasificada generada o proporcionada durante la ejecución del acuerdo de subvención y no podrá desclasificarla sin la autorización por escrito de la autoridad que concede la subvención.

15. La información o el material clasificados de grado RESTREINT UE/EU RESTRICTED deberá almacenarse en mobiliario de oficina con cerradura cuando no se use. Cuando se encuentren en tránsito, los documentos deberán transportarse dentro de un sobre opaco. Los documentos estarán en todo momento en posesión del portador y no se abrirán mientras estén en tránsito.

([4]) La autoridad que concede la subvención deberá introducir las referencias una vez que se hayan adoptado las normas de desarrollo.

([5]) La parte que desee la acreditación deberá remitir a la autoridad que concede la subvención 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.

([6]) Cuando los beneficiarios procedan de Estados miembros que exijan una HPS y/o una HSE para las subvenciones clasificadas de grado RESTREINT UE/EU RESTRICTED, la autoridad que concede la subvención enumerará en la cláusula sobre aspectos de la seguridad estos requisitos de HPS y HSE para los beneficiarios en cuestión.

16. El beneficiario o subcontratista podrá entregar a la autoridad que concede la subvención 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 beneficiario o subcontratista seguirá las instrucciones de seguridad del programa (o proyecto) (ISP) de la Comisión o las normas de desarrollo de la Comisión sobre la seguridad industrial en relación con las subvenciones clasificadas ([7]).

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

18. La acreditación de seguridad del SIC del beneficiario que maneje ICUE de grado RESTREINT UE/EU RESTRICTED y cualquier interconexión de este podrán delegarse en el responsable de seguridad del beneficiario si así lo permiten las disposiciones legales y reglamentarias nacionales. Cuando se delegue la acreditación, las ANS, ASD o las autoridades de acreditación de seguridad (AAS) seguirán siendo responsables de la protección de la información de grado RESTREINT UE/EU RESTRICTED que maneje el beneficiario y seguirán gozando de la facultad de examinar las medidas de seguridad adoptadas por el beneficiario. Además, el beneficiario remitirá a la autoridad que concede la subvención, 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 beneficiario y las interconexiones correspondientes han sido acreditados para el manejo de la ICUE de grado RESTREINT UE/EU RESTRICTED.

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

19. En el apéndice E de la presente cláusula sobre aspectos de la seguridad figuran los requisitos mínimos de los SIC que manejan información clasificada de grado RESTREINT UE/EU RESTRICTED.

CONDICIONES PARA LA SUBSCONTRATACIÓN POR PARTE DEL BENEFICIARIO

20. El beneficiario deberá obtener la autorización de la autoridad que concede la subvención antes de subcontratar cualquier parte de un acuerdo de subvención clasificado.

21. No se podrá autorizar la subcontratación a una entidad registrada en un país que no sea miembro de la UE ni a una entidad perteneciente a una organización internacional si dicho país 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.

22. Cuando el beneficiario subcontrate, las disposiciones de seguridad del acuerdo de subvención serán de aplicación *mutatis mutandis* al subcontratista o subcontratistas y a su personal. En tal caso, corresponderá al beneficiario asegurarse de que todos los subcontratistas apliquen estos principios a sus propios acuerdos de subcontratación. Para garantizar una supervisión adecuada de la seguridad, la autoridad de seguridad de la Comisión notificará a las ANS y/o ASD del beneficiario o subcontratista la subcontratación de todos los subcontratos conexos clasificados de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET. Cuando proceda, se entregará a las ANS y/o ASD del beneficiario y 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 acuerdos de subvención clasificados figuran las ANS y ASD que exigen que se les notifiquen las disposiciones de seguridad de los acuerdos de subvención clasificados de grado RESTREINT UE/EU RESTRICTED ([8]).

23. El beneficiario no podrá revelar ICUE a un subcontratista sin la aprobación previa por escrito de la autoridad que concede la subvención. Si la ICUE debe enviarse a los subcontratistas con frecuencia o de manera rutinaria, la autoridad que concede la subvención podrá dar su aprobación para un período determinado (por ejemplo, doce meses) o para la duración del subcontrato.

([7]) La autoridad que concede la subvención introducirá las referencias una vez que se hayan adoptado estas normas de desarrollo.
([8]) La autoridad que concede la subvención introducirá las referencias una vez que se hayan adoptado estas normas de desarrollo.

VISITAS

Si se aplica el procedimiento de solicitud de visita (SdV) estándar a visitas que impliquen el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, la autoridad que concede la subvención incluirá los apartados 24, 25 y 26 y suprimirá el apartado 27. 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, la autoridad que concede la subvención deberá suprimir los apartados 25 y 26 e incluir únicamente el apartado 27.

24. 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 25 a 27.

[25. 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 deberá 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 autoridad que concede la subvención).

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

[26. 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 deberá haber recibido la autorización de su ANS o ASD.]

[27. 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 al efecto figura en el apéndice C).]

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

29. La instalación que reciba la visita se asegurará de que se lleve un registro de todos los visitantes. En él se recogerán 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 la persona o las personas visitadas. Sin perjuicio de las normas europeas de protección de datos, dichos registros se conservarán durante un período no inferior a cinco años o lo que indiquen las disposiciones legales y reglamentarias nacionales, según proceda.

VISITAS DE EVALUACIÓN

30. La autoridad de seguridad de la Comisión podrá, con la colaboración de las ANS o ASD correspondientes, efectuar visitas a las instalaciones de los beneficiarios o subcontratistas para comprobar que se cumplen los requisitos de seguridad para el manejo de ICUE.

GUÍA DE CLASIFICACIÓN DE SEGURIDAD

31. La guía de clasificación de seguridad contiene una lista de todos los elementos del acuerdo de subvención que estén clasificados o puedan clasificarse durante la ejecución del acuerdo de subvención, 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 acuerdo de subvención y se encuentra en el apéndice B del presente anexo.

Apéndice B

GUÍA DE CLASIFICACIÓN DE SEGURIDAD

[adaptar las partes que procedan dependiendo del objeto del acuerdo de subvención]

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 tratar ___).
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 ([9]).

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

([9]) 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.

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:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

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 ([10]).>

([10]) 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 ([11]).>

([11]) 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 ([12]).>

([12]) 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 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 autoridad de seguridad de la Comisión (que actúa en nombre de las autoridades que conceden la subvención) en relación con la habilitación de seguridad de establecimiento de una instalación que participa en la solicitud y ejecución de subvenciones o subcontratos clasificados.

1.2. La ficha de información sobre la habilitación de seguridad de establecimiento solo es válida si cuenta con el sello de la correspondiente ANS o ASD u otra autoridad competente.

1.3. La ficha de información sobre la habilitación de seguridad de establecimiento 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 habilitación de seguridad de establecimiento de una instalación determinada. La ANS o ASD solicitante debe especificar el motivo de la investigación en el apartado 7 de la sección de solicitud.

1.4. La información que figura en la ficha de información sobre la habilitación de seguridad de establecimiento no suele ser clasificada; en consecuencia, cuando la Comisión y las ANS o ASD correspondientes deban enviarse una ficha de información sobre la habilitación de seguridad de establecimiento, el envío 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 ficha de información sobre la habilitación de seguridad de establecimiento en un plazo de diez días laborables.

1.6. En caso de que se transmita información clasificada o se conceda una subvención o se proceda a una subcontratación 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 detalladas están dirigidas a la ANS o la ASD o a la autoridad que concede la subvención y la autoridad de seguridad de la Comisión que completen la ficha de información sobre la habilitación de seguridad de establecimiento. 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**	La autoridad que concede la subvención selecciona la casilla apropiada para el tipo de solicitud de ficha de información sobre la habilitación de seguridad de establecimiento. 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 comunicación e información 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, los indicadores del proyecto, el número de la convocatoria o la subvención. Indíquense 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 concreto (en nombre de la ANS o ASD) y la fecha de la solicitud en formato numérico (dd/mm/aaaa).
5. **SECCIÓN DE RESPUESTA**	Apartados 1-5: 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 beneficiario 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 la instalación que figura 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 beneficiario o subcontratista, el proceso de obtención de una HSE hasta el grado ..... inclusive, 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), subvención o subcontrato, programa/proyecto, etc.]

.....

ANS/ASD o autoridad que concede la subvención solicitante: Nombre: ..... Fecha: (dd/mm/aaaa).....

RESPUESTA (en un plazo de diez días laborables)

Por la presente se certifica lo siguiente:

1. […] La instalación mencionada cuenta con una HSE hasta el grado […] S-UE/EU-S inclusive

   […] C-UE/EU-C inclusive.

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 ([13]).>

([13]) 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 beneficiario

Consideraciones generales

1. El beneficiario debe asegurarse de que la protección de la información clasificada de grado RESTREINT UE/EU RESTRICTED cumpla los requisitos mínimos de seguridad establecidos en la presente cláusula de seguridad y cualesquiera otros requisitos adicionales aconsejados por la autoridad que concede la subvención o, en su caso, por la Autoridad Nacional de Seguridad (ANS) o la Autoridad de Seguridad Designada (ASD).

2. Corresponde al beneficiario 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. El beneficiario debe 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 beneficiario para almacenar o tratar información clasificada de grado RESTREINT UE/EU RESTRICTED.

7. La acreditación del SIC del beneficiario 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 beneficiario, 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 acuerdo de subvención. 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 de la autoridad que concede la subvención o de la ANS, ASD o AAS pertinentes, el beneficiario debe presentar pruebas del cumplimiento de la cláusula de seguridad del acuerdo de subvención. Si también se solicita una auditoría e inspección de los procesos e instalaciones del beneficiario para garantizar el cumplimiento de estos requisitos, los beneficiarios permitirán a los representantes de la autoridad que concede la subvención, la ANS, la ASD y/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 a los SIC

13. El acceso al SIC del beneficiario que maneje ICUE (información clasificada de la UE) se concederá 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 e 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 con 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 de los SIC deben estar informados de sus responsabilidades y de los procedimientos que han de 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 beneficiario 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 a la autoridad que concede la subvención 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 beneficiario 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 beneficiario o subcontratista. En este caso, el beneficiario debe realizar una evaluación del riesgo para determinar qué requisitos de seguridad adicionales deben aplicarse en el proceso de acreditación de seguridad. El beneficiario remitirá a la autoridad que concede la subvención 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 beneficiario 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 la autoridad que concede la subvención 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 los 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 beneficiario 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 beneficiario 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 beneficiario 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 los 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 a la autoridad que concede la subvención 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 beneficiarios o subcontratistas que manejen información clasificada de grado RESTREINT UE/EU RESTRICTED, y ANS o ASD a las que deben notificarse los acuerdos de subvención clasificados de grado RESTREINT UE/EU RESTRICTED ([1])

Estado miembro	HSE		Notificación a la ANS y/o ASD de un acuerdo de subvención 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**
Lituania	**X**		**X**			**X**
Luxemburgo	**X**		**X**		**X**	
Hungría		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Países Bajos	**X** (solo para acuerdos de subvención y subcontratos en materia de defensa)		**X** (solo para acuerdos de subvención y subcontratos en materia de defensa)			**X**
Austria		**X**		**X**		**X**
Polonia		**X**		**X**		**X**

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

Portugal		**X**		**X**		**X**
Rumanía		**X**		**X**		**X**
Eslovenia	**X**		**X**			**X**
Eslovaquia	**X**		**X**			**X**
Finlandia		**X**		**X**		**X**
Suecia		**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
15, rue des Petits Carmes
1000 Brussels

Teléfono (Secretaría): +32 25014542

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)
   29, Ulitsa Shesti Septemvri
   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 o un acuerdo de subvención clasificados o ejecuten un contrato o un acuerdo de subvención clasificados).

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 - RS3

   Villemombler Str. 76

   53123 Bonn

   Teléfono: +49 228996154028

   Fax: +49 228996152676

   Correo electrónico: dsagermany-rs3@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 – RS2
Villemombler Str. 76
53123 Bonn

Teléfono: +49 228996152401

Fax: +49 228996152603

Correo electrónico: rs2-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, Athens

Teléfono: +30 2106572022, +30 2106572178

Fax: +30 2106527612

Correo electrónico: daa.industrial@hndgs.mil.gr

ESPAÑA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona, 30
28023 Madrid

Teléfono: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

Correo electrónico: nsa-sp@areatec.com

Para la información relativa a los programas clasificados: programas.ons@areatec.com

En materia de habilitaciones personales de seguridad: hps.ons@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, Nicosia

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.lv, 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
Pilaitės pr. 19
LT-06264 Vilnius

Teléfono: +370 70666128

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

Tel.:+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 The Hague

   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 The Hague

   Teléfono: +31 704419407

   Fax: +31 703459189

   Correo electrónico: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria

   Department I/10, Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Teléfono: +43 153115202594

   Correo electrónico: isk@bka.gv.at

2. DSA in the military sphere:

   BMLVS/Abwehramt

   Postfach 2000
   1030 Vienna

   Correo electrónico: abwa@bmlvs.gv.at

POLONIA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw

Teléfono: +48 225857944

Fax: +48 225857443

Correo electrónico: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 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 Bucharest

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 Government

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