ANEXO VI

INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 13.

II. MARCOS QUE REGULAN EL INTERCAMBIO DE INFORMACIÓN CLASIFICADA

2. Cuando el Consejo haya determinado que existe la necesidad de intercambiar información clasificada de forma prolongada,

   — se celebrará un acuerdo de seguridad de la información, o

   — se celebrará un acuerdo administrativo,

   de conformidad con el artículo 13, apartado 2, y las secciones III y IV y sobre la base de una recomendación del Comité de Seguridad.

3. Cuando la ICUE generada a efectos de una operación PCSD deba comunicarse a terceros Estados u organizaciones internacionales que participen en dicha operación, y cuando no exista ninguno de los marcos a que se refiere el punto 2, el intercambio de ICUE con el tercer Estado u organización internacional de que se trate se regulará, conforme a lo dispuesto en la sección V, por:

   — un acuerdo marco de participación,

   — un acuerdo de participación *ad hoc*, o

   — de no existir alguno de estos, un acuerdo administrativo *ad hoc*.

4. En ausencia de uno de los marcos a que se refieren los puntos 2 y 3, y cuando se adopte la decisión de ceder ICUE a un tercer Estado u organización internacional con arreglo a un procedimiento *ad hoc* de carácter excepcional de conformidad con lo dispuesto en la sección VI, se pedirán garantías por escrito al tercer Estado u organización internacional interesado de que mantendrá protegida la ICUE que se le ceda de acuerdo con los principios básicos y las normas mínimas establecidas por la presente Decisión.

III. ACUERDOS DE SEGURIDAD DE LA INFORMACIÓN

5. Los acuerdos de seguridad de la información establecerán los principios básicos y las normas mínimas aplicables al intercambio de información clasificada entre la Unión y un tercer Estado u organización internacional.

6. Los acuerdos de seguridad de la información establecerán las disposiciones técnicas de aplicación que deban convenirse entre las autoridades de seguridad competentes de las instituciones y órganos pertinentes de la Unión y la autoridad de seguridad competente del tercer Estado u organización internacional de que se trate. Dichas disposiciones tendrán debidamente en cuenta el grado de protección que ofrezcan las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional de que se trate. Serán aprobadas por el Comité de Seguridad.

7. Con arreglo a un acuerdo de seguridad de la información, no se intercambiará ICUE por medios electrónicos a menos que se haya previsto explícitamente en el acuerdo o en las disposiciones técnicas de aplicación correspondientes.

8. En los acuerdos sobre seguridad de la información que celebre el Consejo se designará un registro en cada parte como punto principal de entrada y salida para los intercambios de información clasificada.

9. Con el fin de evaluar la eficacia de las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional en cuestión, se efectuarán visitas de evaluación de común acuerdo con el tercer Estado o la organización internacional de que se trate. Dichas visitas se realizarán de conformidad con las disposiciones pertinentes del anexo III y evaluarán:

   a) el marco regulador aplicable para proteger la información clasificada;

   b) las características propias de la política de seguridad y la manera en que se organiza la seguridad en el tercer Estado u organización internacional, que pueden influir en el grado de la información clasificada que pueda intercambiarse;

   c) las medidas y procedimientos de seguridad que se aplican efectivamente, y

   d) los procedimientos de habilitación de seguridad del grado correspondiente al de la ICUE que ha de cederse.

10. El equipo que efectúe la visita de evaluación en nombre de la Unión evaluará si las normas y procedimientos de seguridad en el tercer Estado o la organización internacional son adecuados para ofrecer protección a la ICUE de un determinado nivel.

11. Los resultados de estas visitas se recogerán en un informe que servirá de base al Comité de Seguridad para determinar el grado máximo de la ICUE que podrá intercambiarse en papel o, cuando proceda, de forma electrónica, con el tercero de que se trate, así como las condiciones específicas de dicho intercambio.

12. Deberá ponerse el máximo empeño en realizar una visita completa de evaluación de la seguridad en el tercer Estado u organización internacional de que se trate antes de que el Comité de Seguridad apruebe las disposiciones de aplicación, con objeto de determinar la naturaleza y la eficacia del sistema de seguridad que esté establecido. No obstante, cuando ello no resulte posible, el Comité de Seguridad recibirá un informe lo más completo posible de la Oficina de Seguridad de la SGC, basado en la información de que disponga, en el que se le informará de la normativa de seguridad aplicable y de la manera en que está organizada la seguridad en el tercer Estado o la organización internacional de que se trate.

13. El informe de la visita de evaluación o, en caso de no existir dicho informe, el informe a que se refiere el punto 12, se remitirá al Comité de Seguridad, que deberá considerarlo satisfactorio, antes de que se ceda efectivamente ICUE al tercer Estado o a la organización internacional de que se trate.

14. Las autoridades de seguridad competentes de las instituciones y órganos de la Unión comunicarán al tercer Estado u organización internacional la fecha a partir de la cual la Unión se encontrará en condiciones de ceder información clasificada de la Unión con arreglo al acuerdo, así como el máximo grado de ICUE que pueda intercambiarse en soporte de papel o por medios electrónicos.

15. Si se juzga necesario, se efectuarán visitas de seguimiento, en particular si:

    a) es necesario elevar el grado en que se cede la ICUE, o

    b) se han notificado a la Unión cambios fundamentales en las medidas de seguridad del tercer Estado u organización internacional que puedan afectar al modo en que protege la ICUE, o

    c) se ha producido un incidente grave que implique revelación no autorizada de ICUE.

16. Una vez que el acuerdo de seguridad de la información esté en vigor y se haya intercambiado información clasificada con el tercer Estado o la organización internacional de que se trate, el Comité de Seguridad podrá decidir modificar el grado máximo de la ICUE que podrá ser intercambiada en papel o por medios electrónicos, en particular, como consecuencia de posibles visitas de evaluación ulteriores.

IV. ACUERDOS ADMINISTRATIVOS

17. Cuando exista la necesidad de intercambiar durante largo tiempo información clasificada, en principio, de un grado no superior a RESTREINT UE/EU RESTRICTED con un tercer Estado o una organización internacional y el Comité de Seguridad haya determinado que la otra parte no cuenta con un sistema de seguridad suficientemente desarrollado como para celebrar un acuerdo de seguridad de la información, el Secretario General podrá, previa aprobación del Consejo, celebrar un acuerdo administrativo, en nombre de la SGC, con las autoridades competentes del tercer Estado o la organización internacional.

18. Cuando por motivos operativos urgentes sea necesario establecer rápidamente un marco de intercambio de información clasificada, el Consejo podrá decidir, con carácter excepcional, que se celebre un acuerdo administrativo para el intercambio de información de un grado de clasificación superior.

19. Por regla general, los acuerdos administrativos adoptarán la forma de un canje de notas.

20. Antes de ceder efectivamente ICUE al tercer Estado o la organización internacional de que se trate, se realizará una visita de evaluación con arreglo al punto 9 y se remitirá el correspondiente informe o, en caso de no existir dicho informe, el informe a que se refiere el punto 12, al Comité de Seguridad, que deberá considerarlo satisfactorio.

21. Con arreglo a un acuerdo administrativo, no se intercambiará ICUE por medios electrónicos a menos que se haya establecido explícitamente en el acuerdo.

V. INTERCAMBIO DE INFORMACIÓN CLASIFICADA EN EL CONTEXTO DE LAS OPERACIONES PCSD

22. La participación de terceros Estados o de organizaciones internacionales en operaciones PCSD se rige por acuerdos marco de participación. Los citados acuerdos incluirán disposiciones en materia de cesión de ICUE generada con motivo de operaciones PCSD a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

23. Los acuerdos de participación *ad hoc* celebrados para una operación PCSD específica incluirán disposiciones sobre la cesión de ICUE generada a efectos de dicha operación a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

24. A falta de acuerdo de seguridad de la información, y a la espera de la celebración de un acuerdo de participación, la cesión de ICUE, generada a efectos de la operación, a un tercer Estado u organización internacional participante en la operación, se regulará mediante un acuerdo administrativo que celebrará el Alto Representante o será objeto de una decisión sobre cesión *ad hoc* de conformidad con la sección VI. Con arreglo a dicho acuerdo solo se intercambiará ICUE mientras se siga contemplando la participación del tercer Estado o de la organización internacional. No se podrá intercambiar ICUE de grado superior a RESTREINT UE/EU RESTRICTED para operaciones civiles PCSD y CONFIDENTIEL UE/UE CONFIDENTIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

25. Las disposiciones sobre la información clasificada que deberán figurar en los acuerdos marco de participación, en los acuerdos de participación *ad hoc* y en los acuerdos administrativos *ad hoc* a que se refieren los puntos 22, 23 y 24 establecerán que el tercer Estado u organización internacional afectado deberá garantizar que su personal destinado en comisión de servicio a la operación protegerá la ICUE con arreglo a las normas de seguridad del Consejo y con cualquier otra directriz emitida por las autoridades competentes, incluida la cadena de mando de la operación.

26. Si la Unión y el tercer Estado o la organización internacional contribuyente celebran ulteriormente un acuerdo de seguridad de la información, este acuerdo sustituirá a las disposiciones en materia de intercambio de información clasificada establecidas en cualquier acuerdo marco de participación, acuerdo de participación *ad hoc* o acuerdo administrativo *ad hoc* previo en lo que se refiere al intercambio y manejo de ICUE.

27. No se permitirá el intercambio de ICUE por medios electrónicos con arreglo a un acuerdo marco de participación, un acuerdo de participación *ad hoc* o un acuerdo administrativo *ad hoc* con un tercer Estado u organización internacional, a menos que se haya establecido explícitamente en el acuerdo o en el acuerdo administrativo en cuestión.

28. La ICUE generada a efectos de la operación PCSD podrá ser revelada al personal destinado en comisión de servicio para dicha operación por terceros Estados u organizaciones internacionales de conformidad con lo dispuesto en los puntos 22 a 27. Cuando se conceda autorización de acceso a ICUE en los locales o en los SIC de una operación PCSD a dicho personal, se aplicarán las medidas necesarias (incluida la grabación de la ICUE revelada) para evitar riesgos de pérdida o comprometimiento de la información. Estas medidas se determinarán en los documentos de planificación o de misión.

29. A falta de un acuerdo de seguridad de la información, y en caso de necesidad operativa específica e inmediata, la cesión de ICUE al Estado anfitrión en cuyo territorio se lleve a cabo una operación PCSD podrá regularse mediante un acuerdo administrativo que celebrará el Alto Representante. Esta posibilidad se dispondrá en la decisión que establezca la operación PCSD. La ICUE cedida en esas circunstancias se limitará a la generada para los fines de la operación PCSD y su grado de clasificación no será superior a RESTREINT UE/EU RESTRICTED, salvo que se disponga un grado de clasificación superior en la decisión que establezca la operación PCSD. En el marco del citado acuerdo administrativo, se exigirá al Estado de acogida que se comprometa a proteger la ICUE respetando normas mínimas no menos estrictas que las establecidas por la presente Decisión.

30. A falta de acuerdo de seguridad de la información, la cesión de ICUE a un tercer Estado y a organizaciones internacionales pertinentes, distintos de los participantes en una operación PCSD, podrá regularse mediante un acuerdo administrativo que celebrará la Alta Representante. Si resulta conveniente, se preverá dicha posibilidad y toda condición al respecto en la decisión que establezca la operación PCSD. La ICUE cedida en esas circunstancias se limitará a la generada para los fines de la operación PCSD y su grado de clasificación no será superior a RESTREINT UE/EU RESTRICTED, salvo que se establezca un grado de clasificación superior en la decisión que establezca la operación PCSD. En el marco del citado acuerdo administrativo, se pedirá al tercer Estado o a la organización internacional de que se trate que se comprometan a proteger la ICUE respetando normas mínimas no menos estrictas que las establecidas por la presente Decisión.

31. No será preciso establecer disposiciones de aplicación ni efectuar visitas de evaluación antes de aplicar las disposiciones en materia de cesión de ICUE en el contexto de los puntos 22, 23 y 24.

VI. CESIÓN *AD HOC* CON CARÁCTER EXCEPCIONAL DE ICUE

32. En caso de que no exista un marco de conformidad con las secciones III, IV y V, y cuando el Consejo o uno de sus órganos preparatorios determine que es necesario, a título excepcional, ceder ICUE a un tercer Estado o a una organización internacional, la SGC:

    a) comprobará, en la medida de lo posible, en colaboración con las autoridades de seguridad del tercer Estado u organización internacional de que se trate, que su normativa, estructuras y procedimientos de seguridad garantizan que la ICUE que se les ceda será protegida con arreglo a estándares no menos estrictos que los establecidos por la presente Decisión, e

    b) invitará al Comité de Seguridad a emitir, basándose en la información disponible, una recomendación sobre el grado de confianza que deba concederse a la normativa, estructuras y procedimientos de seguridad del tercer Estado u organización internacional a la que se comunique ICUE.

33. Si el Comité de Seguridad emite una recomendación a favor de la cesión de la ICUE, el asunto se comunicará al Comité de Representantes Permanentes (Coreper), que deberá tomar una decisión sobre la cesión de dicha información.

34. Si la recomendación del Comité de Seguridad no es favorable a la cesión de la ICUE:

    a) para los asuntos relacionados con la PESC o la PCSD, el Comité Político y de Seguridad examinará el asunto y formulará una recomendación al Coreper para que este tome una decisión;

    b) para todos los demás asuntos, el Coreper examinará el asunto y tomará una decisión.

35. Cuando se considere apropiado, y siempre que se cuente con el consentimiento previo por escrito del originador, el Coreper podrá decidir que la información clasificada sea cedida solo en parte o únicamente si se ha reducido el grado de clasificación o se ha desclasificado previamente; o que la información que deba cederse se elabore sin hacer referencia a la fuente o al grado de clasificación UE original.

36. Una vez que se haya tomado la decisión de ceder ICUE, la SGC enviará el documento de que se trate, el cual deberá llevar una marca de posibilidad de cesión que indique a qué tercer Estado u organización internacional ha sido cedido. Antes o en el momento de la cesión efectiva, el tercero de que se trate se comprometerá por escrito a proteger la ICUE que reciba de acuerdo con los principios básicos y las normas mínimas que se establecen en la presente Decisión.

VII. AUTORIDAD PARA CEDER ICUE A TERCEROS ESTADOS U ORGANIZACIONES INTERNACIONALES

37. Cuando exista un marco para el intercambio de información clasificada con un tercer Estado u organización internacional con arreglo al punto 2, el Consejo tomará una decisión que autorice al Secretario General a ceder ICUE al tercer Estado o la organización internacional de que se trate, respetando el principio del consentimiento previo del originador. El Secretario General podrá delegar tal autorización en altos funcionarios de la SGC.

38. Cuando exista un acuerdo de seguridad de la información, con arreglo al punto 2, primer inciso, el Consejo podrá adoptar una decisión que autorice al Alto Representante a ceder al tercer Estado o a la organización internacional de que se trate ICUE originada en el Consejo en el ámbito de la política exterior y de seguridad común, tras haber obtenido el consentimiento del originador de todo material de origen contenido en ella. El Alto Representante podrá delegar tal autorización en altos funcionarios del SEAE o en los Representantes Especiales de la Unión.

39. Cuando exista un marco para el intercambio de información clasificada con un tercer Estado u organización internacional con arreglo a los puntos 2 o 3, se autorizará al Alto Representante a ceder ICUE, de conformidad con la decisión por la que se establezca la operación PCSD y respetando el principio del consentimiento previo del originador. El Alto Representante podrá delegar tal autorización en altos funcionarios del SEAE, en la Operación de la UE, en los Comandantes de la Fuerza o de la Misión, o en los Jefes de Misión de la UE.

Apéndices

Apéndice A

DEFINICIONES

A los efectos de la presente Decisión, se entenderá por:

«Acreditación»: el proceso que concluye con la declaración formal de la Autoridad de Acreditación de Seguridad (AAS) de que un sistema ha recibido la correspondiente aprobación para tratar material de un grado determinado de clasificación en un modo específico de seguridad en su entorno operativo y con un nivel aceptable de riesgo, en el entendimiento de que se aplica un conjunto aprobado de medidas de seguridad técnicas, físicas, de organización y de procedimiento.

«Activos»: todo lo que tenga valor para una organización, para su funcionamiento y continuidad, incluidos los recursos de información disponibles para llevar a cabo su misión.

«Autorización para acceder a ICUE»: una decisión de la autoridad facultada para proceder a los nombramientos de la SGC, adoptada sobre la base de una garantía concedida por una autoridad competente de un Estado miembro, que acredita que un funcionario u otro agente de la SGC o experto nacional destinado en la SGC en comisión de servicio puede tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada, siempre que se haya establecido su necesidad de conocer dicha información y haya sido adecuadamente informado sobre sus responsabilidades.

«Ciclo de vida de un SIC»: la duración completa de la existencia de un SIC, que comprende inicio, concepción, planificación, análisis de requisitos, diseño, desarrollo, pruebas, aplicación, funcionamiento y mantenimiento, y desmantelamiento.

«Contrato clasificado»: el contrato celebrado entre la SGC y un contratista para el suministro de bienes, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique el acceso a ICUE o la creación de dicha información.

«Subcontrato clasificado»: el contrato celebrado por un contratista de la SGC con otro contratista (denominado «subcontratista») para el suministro de bienes, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique el acceso a ICUE o la creación de dicha información.

«Sistema de información y comunicaciones» (SIC) — véase el artículo 10, apartado 2.

«Contratista»: la persona física o jurídica con capacidad legal para celebrar contratos.

«Material de cifra»: algoritmos criptológicos, módulos criptológicos *software* y *hardware,* y productos, incluida la información sobre su uso y la documentación pertinente y los datos de claves.

«Producto criptológico»: producto que tiene como función primordial y principal la prestación de servicios de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, no repudio) mediante uno o varios mecanismos criptológicos.

«Operación PCSD»: una operación militar o civil de gestión de crisis en virtud del título V, capítulo 2, del TUE.

«Desclasificación»: supresión de toda clasificación de seguridad.

«Defensa en profundidad»: la aplicación de una serie de medidas de seguridad organizadas a modo de defensa en barreras sucesivas.

«Autoridad de Seguridad Designada» (ASD): la autoridad responsable ante la Autoridad Nacional de Seguridad (ANS) de un Estado miembro, encargada de comunicar a las sociedades industriales u otro tipo de entidades la política nacional en todos los aspectos de la seguridad industrial y de facilitarles dirección y asistencia para su aplicación. La función de ASD podrá ser ejercida por la ANS o por cualquier otra autoridad competente.

«Documento»: toda información registrada, independientemente de su soporte o características físicas.

«Reducción del grado de clasificación»: reducción del grado de clasificación de seguridad.

«Información clasificada de la UE» (ICUE) — véase el artículo 2, apartado 1.

«Habilitación de seguridad de establecimiento»: la certificación administrativa por parte de una ANS o una ASD de que, desde el punto de vista de la seguridad, un determinado establecimiento puede brindar un nivel adecuado de protección a la ICUE de un grado específico de clasificación de seguridad.

«Manejo» de ICUE: toda intervención posible a la que puede estar sujeta a lo largo de su ciclo de vida la ICUE, es decir: producción, tratamiento, traslado, reducción del nivel de clasificación, desclasificación y destrucción. En relación con los SIC abarca asimismo su recopilación, exposición, transmisión y almacenamiento.

«Poseedor»: persona debidamente autorizada con una probada necesidad de conocer la información, que está en posesión de cualquier ICUE y es, por tanto, responsable de su protección.

«Sociedad industrial u otro tipo de entidad»: una entidad que participa en el suministro de bienes, la ejecución de obras o la prestación de servicios. Puede tratarse de sociedades industriales, comerciales y de servicios o de centros científicos, de investigación, educativos y de desarrollo, o de individuos que trabajen por cuenta propia.

«Seguridad industrial» — véase el artículo 11, apartado 1.

«Garantía de la información» — véase el artículo 10, apartado 1.

«Interconexión» — véase el anexo IV, punto 32.

«Tratamiento de la información clasificada» — véase el artículo 9, apartado 1.

«Material»: todo documento, soporte de datos, máquina o aparato, producido o en proceso de producción.

«Originador»: la institución, organismo o agencia de la Unión, el Estado miembro, el tercer Estado o la organización internacional bajo cuya autoridad se ha producido información clasificada o se ha introducido en las estructuras de la Unión.

«Seguridad en el personal» — véase el artículo 7, apartado 1.

«Habilitación personal de seguridad» (HPS): la declaración de una autoridad competente de un Estado miembro, efectuada al término de una investigación de seguridad realizada por las autoridades competentes del Estado miembro, mediante la cual se acredita que una persona puede tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada.

«Certificado de habilitación personal de seguridad» (CHPS): el certificado expedido por una autoridad competente mediante el cual se establece que una persona está habilitada y dispone de un certificado de habilitación de seguridad o una autorización válidos para acceder a ICUE expedidos por la autoridad facultada para proceder a los nombramientos, y que indica el grado de ICUE a que puede tener acceso (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), el período de validez de la habilitación y la fecha de caducidad del propio certificado.

«Seguridad física» — véase el artículo 8, apartado 1.

«Instrucciones de seguridad de un programa o proyecto»: lista de procedimientos de seguridad aplicables a un programa o proyecto específico para tipificar los procedimientos de seguridad. Puede ser objeto de revisión a lo largo de la ejecución del programa o proyecto.

«Inscripción en un registro» — véase el anexo III, punto 18.

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

«Riesgo»: la posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades internas o externas de una organización o de cualquier sistema que esta utilice y al hacerlo ocasione daños a la organización o a sus activos tangibles o intangibles. Se mide como la combinación de la probabilidad de que se cumplan las amenazas y de su repercusión.

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

— «Evaluación del riesgo»: consiste en determinar las amenazas y las vulnerabilidades, y llevar a cabo el correspondiente análisis del riesgo, es decir, el análisis de la probabilidad y de las repercusiones.

— «Comunicación del riesgo»: consiste en sensibilizar de los riesgos a las comunidades de usuarios de SIC, informar de tales riesgos a las autoridades responsables de la aprobación y a las autoridades operativas.

— «Tratamiento del riesgo»: consiste en atenuar, suprimir o reducir el riesgo (adoptando una combinación adecuada de medidas técnicas, físicas, de gestión o de procedimiento), transferir el riesgo o hacer un seguimiento del mismo.

«Cláusula sobre aspectos de la seguridad»: conjunto de condiciones contractuales especiales impuestas por la autoridad contratante y que forman parte integrante de un contrato clasificado que conlleve el acceso a ICUE o la creación de ese tipo de información; en ella se enumeran los requisitos de seguridad o los elementos del contrato que requieren protección de seguridad.

«Guía de clasificación de seguridad»: documento que describe los elementos de un programa o contrato que están clasificados, con especificación de los grados de clasificación de seguridad aplicables. La guía de clasificación de seguridad podrá ampliarse durante toda la vigencia del programa o contrato, y se podrá reducir el grado de clasificación o reclasificar los elementos de información; cuando exista una guía de clasificación de seguridad, formará parte de la cláusula sobre aspectos de la seguridad.

«Investigación de seguridad»: procedimiento de investigación efectuado por la autoridad competente de un Estado miembro con arreglo a las disposiciones legales y reglamentarias nacionales vigentes, con el fin de obtener la garantía de que no se conocen datos desfavorables que impidan conceder a una persona determinada una HPS o una autorización para acceder a ICUE de un determinado nivel (CONFIDENTIEL UE/EU CONFIDENTIAL o superior).

«Modo de operación de seguridad»: el conjunto de las condiciones de funcionamiento de un SIC, definidas sobre la base de la clasificación de la información manejada y de los grados de habilitación, las aprobaciones formales de acceso y la necesidad de conocer de los usuarios. Existen cuatro modos de operación para el manejo y la transmisión de información clasificada: dedicado, unificado a nivel superior, compartimentado y multinivel.

— «Modo dedicado»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él y tienen la misma necesidad de conocer toda la información manejada en el SIC.

— «Modo unificado a nivel superior»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, pero en el que no todas las personas con acceso al SIC tienen la misma necesidad de conocer la información manejada en él; la aprobación para acceder a la información puede darla una persona.

— «Modo compartimentado»: modo de operación en el que todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, pero no todas las personas con acceso al SIC poseen una autorización formal de acceso a toda la información manejada en él; la autorización formal supone, a diferencia del acceso que se concede a discreción de una persona, la existencia de una gestión formal centralizada del control de acceso.

— «Modo multinivel»: modo de operación en el que no todas las personas con acceso al SIC están habilitadas al grado más alto de clasificación de la información manejada en él, y no todas las personas con acceso al SIC tienen la misma necesidad de conocer la información manejada en él.

«Proceso de gestión del riesgo de seguridad»: la totalidad del proceso de determinación, control y disminución de acontecimientos inciertos que puedan afectar a la seguridad de una organización o de cualquiera de los sistemas que utiliza. Abarca todas las actividades relacionadas con los riesgos, incluida la evaluación, tratamiento, aceptación y comunicación.

«TEMPEST»: la investigación, estudio y control de las emanaciones electromagnéticas comprometedoras y las medidas para suprimirlas.

«Amenaza»: la posible causa de un incidente no deseado que pueda ocasionar daños a una organización o a algunos de los sistemas que use; las amenazas pueden ser accidentales o deliberadas (maliciosas) y constan de elementos amenazadores, posibles blancos y métodos de ataque.

«Vulnerabilidad»: una debilidad, cualquiera que sea su naturaleza, que pueda ser aprovechada por una o varias amenazas. La vulnerabilidad puede resultar de una omisión o guardar relación con una deficiencia en el grado, completitud o coherencia de los controles, y puede ser técnica, física, de procedimiento, de organización o de funcionamiento.

Apéndice B

CORRESPONDENCIA DE LAS CLASIFICACIONES DE SEGURIDAD

| UE | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |

| Bélgica | Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998) | Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998) | Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998) | nota (1) *[infra]* |

| Bulgaria | Строго секретно | Секретно | Поверително | За служебно ползване |

| República Checa | Přísně tajné | Tajné | Důvěrné | Vyhrazené |

| Dinamarca | YDERST HEMMELIGT | HEMMELIGT | FORTROLIGT | TIL TJENESTEBRUG |

| Alemania | STRENG GEHEIM | GEHEIM | VS (2) — VERTRAULICH | VS — NUR FÜR DEN DIENSTGEBRAUCH |

| Estonia | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |

| Irlanda | Top Secret | Secret | Confidential | Restricted |

| Grecia | Άκρως Απόρρητο Abr: ΑΑΠ | Απόρρητο Abr: (ΑΠ) | Εμπιστευτικό Abr: (ΕΜ) | Περιορισμένης Χρήσης Abr: (ΠΧ) |

| España | SECRETO | RESERVADO | CONFIDENCIAL | DIFUSIÓN LIMITADA |

| Francia | Très Secret Défense | Secret Défense | Confidentiel Défense | nota (3) infra |

| Croacia | VRLO TAJNO | TAJNO | POVJERLJIVO | OGRANIČENO |

| Italia | Segretissimo | Segreto | Riservatissimo | Riservato |

| Chipre | Άκρως Απόρρητο Abr: (ΑΑΠ) | Απόρρητο Abr: (ΑΠ) | Εμπιστευτικό Abr: (ΕΜ) | Περιορισμένης Χρήσης Abr: (ΠΧ) |

| Letonia | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |

| Lituania | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |

| Luxemburgo | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |

| Hungría | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |

| Malta | L-Ogħla Segretezza | Sigriet | Kunfidenzjali | Ristrett |

| Top Secret | Secret | Confidential | Restricted (4) |

| Países Bajos | Stg. ZEER GEHEIM | Stg. GEHEIM | Stg. CONFIDENTIEEL | Dep. VERTROUWELIJK |

| Austria | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |

| Polonia | Ściśle tajne | Tajne | Poufne | Zastrzeżone |

| Portugal | Muito Secreto | Secreto | Confidencial | Reservado |

Rumanía | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |

Eslovenia | STROGO TAJNO | TAJNO | ZAUPNO | INTERNO |

Eslovaquia | Prísne tajné | Tajné | Dôverné | Vyhradené |

Finlandia | ERITTÄIN SALAINEN YTTERST HEMLIG | SALAINEN HEMLIG | LUOTTAMUKSELLINEN KONFIDENTIELL | KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG |

Suecia ([5]) | HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET HEMLIG | HEMLIG/CONFIDENTIAL HEMLIG | HEMLIG/RESTRICTED HEMLIG |

Reino Unido | UK TOP SECRET | UK SECRET | nota ([6]) infra | UK OFFICIAL-SENSITIVE |

([1]) Diffusion restreinte/Beperkte Verspreiding no constituye una clasificación de seguridad en Bélgica. Bélgica maneja y protege la información "RESTREINT UE/EU RESTRICTED" con un rigor no inferior al de las reglas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

([2]) Alemania: VS = Verschlusssache.

([3]) Francia no utiliza la clasificación "RESTREINT" en su sistema nacional. Francia maneja y protege la información "RESTREINT UE/EU RESTRICTED" con un rigor no inferior al de las reglas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

([4]) En Malta, las marcas en maltés e inglés pueden utilizarse indistintamente.

([5]) Suecia: Las marcas de clasificación de seguridad indicadas en la línea superior son utilizadas por las autoridades de defensa, y las indicadas en la línea inferior las utilizadas por otras autoridades.

([6]) El Reino Unido no utiliza ya la clasificación "UK CONFIDENTIAL" en su sistema nacional. El Reino Unido trata y protege la información clasificada "CONFIDENTIEL UE/EU CONFIDENTIAL" con arreglo a los requisitos de protección de seguridad correspondientes a "UK SECRET".».

Apéndice C

LISTA DE AUTORIDADES NACIONALES DE SEGURIDAD (ANS)

BÉLGICA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. de la Secretaría: +32 25014542
Fax +32 25014596
Correo electrónico: nvo-ans@diplobel.fed.be

BULGARIA
State Commission on Information Security
90 Cherkovna Str.
1505 Sofía

Tel. +359 29333600
Fax +359 29873750
Correo electrónico: dksi@government.bg
Página web: www.dksi.bg

REPÚBLICA CHECA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel. +420 257283335
Fax +420 257283110
Correo electrónico: czech.nsa@nbu.cz
Página web: www.nbu.cz

DINAMARCA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel. +45 33325566
Fax +45 33931320

ALEMANIA
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin

Tel. +49 30186810
Fax +49 30186811441
Correo electrónico: oesIII3@bmi.bund.de

ESTONIA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel. +372 717 0019, +372 7170117
Fax +372 7170213
Correo electrónico: nsa@mod.gov.ee

IRLANDA
National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2

Tel. +353 14780822
Fax +353 14082959

GRECIA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Counter Intelligence and Security Directorate (NSA)
227-231 HOLARGOS
STG 1020 ATHENS

Tel. +30 2106572045
+30 2106572009
Fax +30 2106536279
+30 2106577612

ESPAÑA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel. +34 913725000
Fax +34 913725808
Correo electrónico: nsa-sp@areatec.com

FRANCIA
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

Tel. +33 171758177
Fax +33 171758200

CROACIA
Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia

Tel. +385 14681222
Fax +385 14686049
www.uvns.hr

ITALIA
Presidenza del Consiglio dei Ministri
D.I.S.-U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tel. +39 0661174266
Fax +39 064885273

CHIPRE
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tel. +357 22807569, +357 22807643, +357 22807764
Fax +357 22302351
Correo electrónico: cynsa@mod.gov.cy

LETONIA
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga

Tel. +371 67025418
Fax +371 67025454
Correo electrónico: ndi@sab.gov.lv

LITUANIA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Tel. +370 706 66701, +370 706 66702
Fax +370 706 66700
Correo electrónico: nsa@vsd.lt

LUXEMBURGO
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tel. +352 24782210 central
+352 24782253 direct
Fax +352 24782243

HUNGRÍA
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 (1) 7952303
Fax +36 (1) 7950344
Postal address:
H-1357 Budapest, PO Box 2
Correo electrónico: nbf@nbf.hu
Página web: www.nbf.hu

MALTA
Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta

Tel. +356 21249844
Fax +356 25695321

PAÍSES BAJOS
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel. +31 703187060
Fax +31 703187522

AUSTRIA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tel. +43 1531152594
Fax +43 1531152615
Correo electrónico: ISK@bka.gv.at

POLONIA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa

Tel. +48 225857360
Fax +48 225858509
Correo electrónico: nsa@abw.gov.pl
Página web: www.abw.gov.pl

ESLOVAQUIA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel. +421 268692314
Fax +421 263824005
Página web: www.nbusr.sk

PORTUGAL
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel. +351 213031710
Fax +351 213031711

FINLANDIA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Teléfono 1: +358 160505890
Fax +358 916055140
Correo electrónico: NSA@formin.fi

RUMANÍA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
Strada Mures nr. 4012275 Bucharest

Tel. +40 212245830
Fax +40 212240714
Correo electrónico: nsa.romania@nsa.ro
Página web: www.orniss.ro

SUECIA
Utrikesdepartementet
(Ministry for Foreign Affairs)
UD-RS
S-103 39 Stockholm

Tel. +46 84051000
Fax +46 87231176
Correo electrónico: ud-nsa@foreign.ministry.se

ESLOVENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel. +386 14781390
Fax +386 14781399
Correo electrónico: gp.uvtp@gov.si

REINO UNIDO
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Teléfono 1: +44 2072765645
Teléfono 2: +44 2072765497
Fax +44 2072765651
Correo electrónico: UK-NSA@cabinet-office.x.gsi.gov.uk

Apéndice D

LISTA DE ABREVIATURAS

Acrónimo	Significado
AAS	Autoridad de Acreditación de Seguridad
ACC	Autoridad de Certificación Criptológica
ADA	Autoridad debidamente acreditada
ADC	Autoridad de Distribución Criptológica
AGI	Autoridad de Garantía de la Información
ANS	Autoridad Nacional de Seguridad
ASD	Autoridad de Seguridad Designada
CCTV	Circuito cerrado de televisión
CHPS	Certificado de habilitación personal de seguridad
Coreper	Comité de Representantes Permanentes
ECSD	Dirección de Seguridad de la Comisión Europea
GI	Garantía de la Información
HPS	Habilitación personal de seguridad
ICUE	Información clasificada de la UE
PCSD	Política Común de Seguridad y Defensa
PESC	Política Exterior y de Seguridad Común
REUE	Representante Especial de la UE
SDI	Sistema de detección de intrusiones
SGC	Secretaría General del Consejo
SIC	Sistemas de información y comunicaciones que manejen ICUE
TI	Tecnologías de la información