ANEXO II.

PROCEDIMIENTO DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA

PR20

INDICE

1. OBJETO

1. El objeto del presente documento es la definición del Procedimiento aplicable a la Clasificación y Tratamiento de la Información Clasificada manejada por el <<ORGANISMO>>, con independencia del soporte en el que se encuentre: papel o dispositivos electrónicos.

Aunque el artículo 3 del Real Decreto, 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS), excluye de su ámbito de aplicación los sistemas que tratan información clasificada, redirigiendo su regulación a la Ley 9/1968, de 5 de abril, de Secretos Oficiales y su normativa de desarrollo, entendemos que es muy importante que los organismos de las AA.PP. españolas posean información suficiente para, en primera instancia, **identificar y tratar adecuadamente Información Clasificada** y, en segunda instancia, y cuando ello sea posible, **aprovechar el marco de seguridad impuesto por el ENS**, posibilitando la compartición de esfuerzos y la mejora en la eficiencia de las medidas de seguridad adoptadas.

Por todo ello, cuando proceda y resulte de aplicación, se complementará la implantación del presente Procedimiento atendiendo al **nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas del <<ORGANISMO>>,** que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ÁMBITO DE APLICACIÓN

2. Este Procedimiento es de aplicación a todo el ámbito de actuación del <<ORGANISMO>>, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad del <<ORGANISMO>>.
3. El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal del <<ORGANISMO>> que trate Información Clasificada y que, de manera permanente o eventual, preste sus servicios en el <<ORGANISMO>>, incluyendo el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información del <<ORGANISMO>> en el sentido descrito.
4. En el ámbito del presente Procedimiento, se entiende por usuario cualquier empleado público perteneciente o ajeno al <<ORGANISMO>>, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el <<ORGANISMO>> y que utilice o posea acceso a los Sistemas de Información del <<ORGANISMO>>.

3. VIGENCIA

5. El presente Procedimiento ha sido aprobado por la <<U/OC>> del <<ORGANISMO>>, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que el <<ORGANISMO>> pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.
6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del <<ORGANISMO>>.
7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este Procedimiento.

4. REVISIÓN Y EVALUACIÓN

8. La gestión interna en el <<ORGANISMO>> de este Procedimiento corresponde a la <<U/OC>>, que es competente para:
    - Interpretar las dudas que puedan surgir en su aplicación.
    - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
    - Verificar su efectividad.
9. Anualmente (o siempre que existen circunstancias que así lo aconsejen), la <<U/OC>> revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> del <<ORGANISMO>>.
10. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.
11. Será la <<U/OC>> de seguridad competente del <<ORGANISMO>> la encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. Las referencias que se han tenido en cuenta para la redacción de este Procedimiento han sido:
    - Ley 9/1968, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales.
    - Decreto 242/1969, de 20 de Febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

- Decisión 2011/292/UE, de 31 de marzo, Normas de seguridad para la protección de la Información Clasificada de la UE.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- Orden PRE/2130/2009, de 31 de julio. Autoridad Delegada para la Seguridad de la Información Clasificada OTAN/UE/UEO.
- Orden PRE/3289/2006, de 23 de octubre. Autoridad Delegada para la Seguridad de la Información Clasificada ESA.
- Norma NS/02 Seguridad en el Personal – Habilitación de Seguridad del Personal, de la Autoridad Delegada para la Seguridad de la Información Clasificada.
- Norma NS/04 Seguridad de la Información, de la Autoridad Delegada para la Seguridad de la Información Clasificada.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Documentos y Guías CCN-STIC.

6. TAXONOMÍA DE LA INFORMACIÓN

6.1. INFORMACIÓN E INFORMACIÓN CLASIFICADA

Conceptos Básicos[1]

- **Información** es todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.
- **Información Clasificada** es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.
- **Documentación Clasificada** es cualquier soporte que contenga Información Clasificada registrada, en cualquier formato físico (escrito, impreso, cinta, fotografía, mapa, dibujo, esquema, nota, soporte informático, óptico o vídeo, etc.). La más tradicional es en formato papel, aunque cada día se hace un uso más extensivo de los soportes informáticos.
- **Material Clasificado** engloba cualquier documentación, pieza, equipo, programa, desarrollo, armamento, sistema o similar, fabricado o en proceso de fabricación, cuyo conocimiento necesite protección frente a difusión no autorizada. Es un concepto más amplio que el de documentación clasificada, pero menos que el de

[1] Definiciones tomadas de la Norma "NS-04 Seguridad de la Información", de la Autoridad Delegada para la Seguridad de la Información Clasificada.

Información Clasificada, dado que no incluye, por ejemplo, a la Información Clasificada en las personas (almacenada en la mente o comunicada verbalmente).

Materias Clasificadas

13. Definidas en la Ley 9/1968, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales (en adelante LSO), como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado, y que se califican en las categorías de **SECRETO** y **RESERVADO**, en atención al grado de protección que requieren, según se definen en el Anexo I del presente Procedimiento.

Materias Objeto de Reserva Interna[2]

14. Se definen como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda afectar a la seguridad del Estado, amenazar sus intereses o dificultar el cumplimiento de su misión. Se clasifican en las categorías de **CONFIDENCIAL** y **DIFUSIÓN LIMITADA**, en atención al grado de protección que requieren, según se definen en el Anexo I del presente Procedimiento.

6.2. CUSTODIA DE LA INFORMACIÓN CLASIFICADA

15. A lo largo de su ciclo de vida, la Información Clasificada estará asignada a un responsable de su custodia (órgano, organismo o persona), que podrá ser sustituido, pero que siempre deberá existir. Dicho **custodio** manejará y cederá la información bajo su custodia conforme a la normativa establecida por el Responsable de la Información o acordada con el mismo y de conformidad con el ordenamiento jurídico vigente.

16. Cuando el custodio sea también quien almacena la información, podrá recibir el nombre de **depositario**.

6.3. USUARIO DE LA INFORMACIÓN CLASIFICADA

17. El usuario es la persona que, en el cumplimiento de sus funciones, tiene que acceder a la Información Clasificada y, en consecuencia, deberá estar debidamente autorizado, comprometiéndose a cumplir los requisitos de acceso a la misma.

18. La condición de usuario no implica ningún derecho o prerrogativa especial sobre la propiedad de la Información Clasificada. El usuario tendrá la custodia de la Información Clasificada en tanto acceda a la misma o esté asignada a su cargo.

19. El usuario asume las siguientes responsabilidades:

    - Proteger adecuadamente la Información Clasificada a su cargo.

[2] Cuyos precedentes pueden encontrarse en la Política de Seguridad de la Información del Ministerio de Defensa, en los Acuerdos para la Protección de la Información Clasificada con otros países y en diversas Políticas de Seguridad de Organizaciones Internacionales.

- Conocer y cumplir la normativa nacional y las normas específicas de seguridad del <<ORGANISMO>> referentes a la protección de la Información Clasificada.
- Mantener la debida reserva ante terceros sobre su condición de titular de una Habilitación Personal de Seguridad.
- No manejar Información Clasificada al margen de los canales formalmente establecidos (Infraestructura Nacional de Protección).
- Cooperar con el Responsable de Seguridad del <<ORGANISMO>> o la <<U/OC>> competente en la materia del <<ORGANISMO>>, en todo aquello que se relacione con la seguridad de la Información Clasificada en su puesto de trabajo, en su entorno laboral y en las actividades y foros en que intervenga.
- Mantener la reserva sobre la Información Clasificada a la que pudiera haber tenido, incluso una vez haya caducado su Habilitación Personal de Seguridad.

6.4. ACCESO A LA INFORMACIÓN CLASIFICADA

20. El acceso de un usuario a la Información Clasificada se realizará conforme a las condiciones que se especifiquen en las regulaciones y normas que resulten de aplicación3, donde podrá determinarse autorizar dicho acceso si el usuario:
    - Posee una Habilitación Personal de Seguridad (HPS) adecuada, si el acceso es a Información Clasificada de grado CONFIDENCIAL o superior.
    - Se ha determinado su "Necesidad de Conocer", y
    - Ha recibido la preceptiva formación de seguridad.
21. En cualquier caso, la <<U/OC>> del <<ORGANISMO>> tiene la potestad para no autorizar el acceso, aun cuando se den las condiciones necesarias anteriores, si estima o aprecia que pueda existir un riesgo no aceptable para la seguridad de la información.
22. Las personas que sólo necesiten acceder a información con clasificación DIFUSIÓN LIMITADA deberán haber sido instruidas en sus responsabilidades de seguridad y habrán de tener "Necesidad de conocer". No se necesitará HPS para acceder a la información con clasificación de dicho grado.

7. PROPIEDAD DE LA INFORMACIÓN

23. En general, la información tendrá un órgano/organismo originador, bajo cuya autoridad o tutela se genera. El órgano/organismo originador definirá quién ostenta la propiedad inicial de dicha información.
24. Además, en sintonía con lo dispuesto en el ENS, cada información tratada por el <<ORGANISMO>> tendrá un Responsable de la Información (propietario de la

[3] En concreto, "Norma NS-02 Seguridad en el Personal – Habilitación de Seguridad del Personal", de la Autoridad Delegada para la Seguridad de la Información Clasificada.

información) claramente establecido en la Política de Seguridad de la Información del <<ORGANISMO>>, que podrá o no coincidir con el antedicho órgano/organismo originador.

25. El Responsable de la Información es el que define las reglas por las que se rige su tratamiento y su nivel de seguridad, en línea con lo dispuesto en el ENS y en el resto del ordenamiento jurídico de aplicación, y define los criterios para que pueda producirse una transferencia de la propiedad, si se admite esa posibilidad.
26. La propiedad de la información puede ser transferida. No debe confundirse con la distribución o la cesión de información, que no implica un cambio de propietario de la misma, sino únicamente de custodio.

8. LA CLASIFICACIÓN DE LA INFORMACIÓN

8.1 CONCEPTOS GENERALES

27. Por Clasificación se entiende el acto formal por el cual la **Autoridad de Clasificación** asigna a una información un grado de clasificación, en atención al riesgo que supone su revelación no autorizada para la seguridad y defensa del Estado o sus intereses, y con la finalidad de protegerla.
28. Según se determina en el artículo 2 de la Ley 9/1968, de Secretos Oficiales, tendrán carácter de Información Clasificada, sin necesidad de previa clasificación, las materias que así sean declaradas por ley.
29. Una vez asignado el grado de clasificación a una determinada información, se marcará sobre el soporte de la misma, de forma adecuada y claramente visible.
30. Las clasificaciones de seguridad y el marcado de la Información Clasificada, en cada caso, se aplicarán de conformidad con la normativa de seguridad que le sea de aplicación y en las condiciones que en la misma se establezcan.
31. **Reclasificación** es el acto formal por el cual la Autoridad de Clasificación modifica el grado de clasificación de una Información Clasificada.
32. **Desclasificación** es el acto formal por el cual la Autoridad de Clasificación retira todo grado de clasificación asignado previamente a una información.

8.2 GRADOS DE CLASIFICACIÓN

33. La Información Clasificada se graduará de conformidad con la normativa que resulte de aplicación en cada momento.
34. Según la normativa europea de aplicación en España, la Información Clasificada puede poseer uno de los siguientes cuatro grados: **SECRETO, RESERVADO, CONFIDENCIAL** y **DIFUSIÓN LIMITADA**.
35. La **Autoridad de Clasificación** es el órgano superior con potestad para proceder a la clasificación de la Información Clasificada de origen nacional.

36. El **órgano/organismo originador** (o el Responsable de la Información) es responsable de proponer la clasificación de seguridad de la información y su difusión inicial.

37. Una vez aprobado por la Autoridad de Clasificación el grado de clasificación de la Información Clasificada, no podrá alterarse, reducirse ni eliminarse sin el consentimiento del órgano/organismo originador. En el momento de su creación, los órganos/organismos originadores indicarán, siempre que esta posibilidad exista, si el grado de clasificación de la información puede reducirse o eliminarse en cierta fecha o bajo ciertos supuestos. Es prerrogativa del órgano/organismo originador proponer a la Autoridad de Clasificación la modificación de la clasificación de seguridad durante su ciclo de vida.

38. Como se señala en el Anexo I del presente Procedimiento, los grados de clasificación nacional en España son, de mayor a menor, los siguientes:

- **SECRETO (S)**
- **RESERVADO (R)**[4]
- **CONFIDENCIAL (C)**
- **DIFUSIÓN LIMITADA (DL)**[5]

39. Su significado y criterios de uso se definen en el citado Anexo I.[6]

8.3 CAPACIDAD PARA CLASIFICAR

Autoridad de Clasificación

40. La capacidad para clasificar es exclusiva de las Autoridades de Clasificación, pudiendo únicamente delegarse dicha capacidad cuando la normativa de seguridad así lo contemple.

[4] Los grados SECRETO y RESERVADO están definidos en la LSO.
[5] Los grados CONFIDENCIAL y DIFUSIÓN LIMITADA están definidos en la norma "NS-04 Seguridad de la Información", de la Autoridad Delegada para la Seguridad de la Información Clasificada, así como en Políticas de Seguridad de Organizaciones Internacionales y Acuerdos para Protección de la Información Clasificada.
[6] Todos los grados anteriores han sido determinados en la Decisión 2011/292/UE del Consejo, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la Información Clasificada de la Unión Europea.

Ámbito Nacional

41. En el ámbito nacional, la facultad para clasificar información está atribuida a las Autoridades siguientes:

Clasificación	Autoridad	Características de la facultad de clasificación
SECRETO	• Consejo de Ministros. • Junta de Jefes de Estado Mayor	• Atribución concedida en la LSO. • No puede ser transferida ni delegada • La LSO no contempla grados inferiores.
RESERVADO		
CONFIDENCIAL	• Los Ministros, Secretarios de Estado y Subsecretarios, en sus respectivos Departamentos. • Jefe del Estado Mayor de la Defensa. • Jefe del Estado Mayor del Ejército. • Almirante Jefe del Estado Mayor de la Armada. • Jefe del Estado Mayor del Ejército del Aire.	• Facultad para clasificar en el ámbito de su competencia. • Puede delegarse oficialmente tal competencia. • Las Autoridades de Clasificación tendrán las siguientes atribuciones: - Aprobar o desestimar las Propuestas de Clasificación. - Emitir la Diligencia de Clasificación. - Modificar el grado de clasificación de la información o su plazo de vigencia. - Disponer las Directivas de Clasificación. - Delegar la facultad de clasificación.
DIFUSIÓN LIMITADA		

Ámbito Internacional

42. Las Organizaciones Internacionales establecen en su normativa la necesidad de seguir unos criterios restrictivos al asignar esta función y delegan la responsabilidad de designar a las Autoridades de Clasificación en los responsables de los Componentes Militares y Agencias (caso de OTAN), o en los Directores Generales (caso del Consejo de la UE, Comisión Europea o Agencia Espacial Europea), y en los propios Estados miembro. No establecen diferencias en este sentido en cuanto al grado de clasificación.

43. En este sentido, en España, como Estado miembro, las Autoridades de Clasificación para estos ámbitos han de ser las mismas que las establecidas en el ámbito nacional para cada grado de clasificación equivalente, y con las mismas prerrogativas de delegación.

8.4 PROCEDIMIENTO DE CLASIFICACIÓN, RECLASIFICACIÓN Y DESCLASIFICACIÓN

44. El <<ORGANISMO>> que considere que una determinada información debe ser protegida de su revelación no autorizada, deberá iniciar un proceso de clasificación mediante la confección de la correspondiente **Propuesta de Clasificación**, que será presentada a la Autoridad de Clasificación, al objeto de obtener su aprobación mediante la emisión de la correspondiente Diligencia de Clasificación.

45. La **Propuesta de Clasificación** es el documento por el que se somete a la aprobación de la Autoridad de Clasificación correspondiente una asignación de un grado de clasificación y su vigencia a informaciones individuales o agrupadas.

46. La **Diligencia de Clasificación** es el documento mediante el cual la Autoridad de Clasificación certifica la aprobación de una Propuesta de Clasificación y se definen las condiciones de aplicación de la misma.

47. La **Guía de Clasificación** es el documento que enumera y describe los elementos clasificados de un asunto, Contrato o Programa Clasificado, con especificación de los grados de clasificación asignados a cada uno de ellos. Recoge los datos relevantes de la Información Clasificada (grados de clasificación, vigencias, autoridades que la han clasificado, etc.), y sirve de referencia para el marcado de los documentos.

48. La **Directiva de Clasificación** es el documento mediante el cual la Autoridad de Clasificación asigna un grado de clasificación a la información que, por su naturaleza, y a juicio de la citada Autoridad, no requiera la elaboración de la Propuesta de Clasificación, constituyéndose formalmente en Diligencia de Clasificación de la misma.

49. El proceso para la clasificación de una información constará de los siguientes pasos:

    a) Decisión del ámbito.
    b) Elaboración de la Guía de Clasificación, cuando así se requiera.
    c) Preparación de la Propuesta de Clasificación.
    d) Elevación de la Propuesta de Clasificación.
    e) Formalización de la Diligencia de Clasificación.
    f) Anotación en el Registro de Informaciones Clasificadas y marcado.
    g) Emisión de las Directivas de Clasificación.

50. Al objeto de facilitar el proceso de clasificación, las Autoridades de Clasificación pueden aprobar Directivas de Clasificación, estableciendo que determinados asuntos, materias o elementos, por su especial naturaleza o contenido, se clasificarán previamente, de forma que cualquier información que incluyan deberá clasificarse con el grado indicado.
51. Cuando exista una Directiva de Clasificación o Guía de Clasificación ya aprobada en una anterior Diligencia de Clasificación, que sea pertinente a la información que se propone para su clasificación, el procedimiento se simplifica, bastando con su anotación en el Registro de Informaciones Clasificadas y su marcado.
52. Un procedimiento específico determinará en detalle el proceso de clasificación completo.
53. La Información Clasificada originada en España se constituirá como Información Clasificada Nacional y, por tanto, se propondrá su clasificación conforme a los grados de clasificación establecidos en España, con independencia del destinatario. De este modo, se indicará de forma explícita que España es la propietaria y originadora de esa Información Clasificada.

    Sólo se harán propuestas de uso de marcas de clasificación no nacionales cuando se elabore Información Clasificada en el marco de una operación, programa, proyecto, u otra colaboración específica. En este caso, la información deberá elaborarse conforme a los requisitos establecidos en el Acuerdo para la Protección de Información Clasificada aplicable, en cuanto a idiomas oficiales admitidos, criterios de marcado, identificación del documentos, paginado, etc.
54. Los mensajes o escritos de remisión que pueden acompañar a documentos anexos clasificados con marcas de clasificación no nacionales y tengan entidad propia, podrán ir en idioma diferente, no debiendo contener Información Clasificada. Aunque lleven la clasificación que les corresponda por agregación, dicha marca incluirá una indicación de que el citado escrito no constituye Información Clasificada cuando se separen de los anexos.
55. Se establecerá un procedimiento operativo para la reclasificación y desclasificación de la información. La Autoridad de Clasificación podrá señalar en la Diligencia de Clasificación el tiempo de vigencia del grado de clasificación que ha otorgado a la información, o las circunstancias que lo condicionen, así como mantener o modificar dicho grado o desclasificar la información.

8.5 REGISTRO DE CLASIFICACIONES

56. El procedimiento de clasificación nacional impondrá la obligación de anotar en un Registro de Informaciones Clasificadas todas las decisiones adoptadas respecto a la clasificación de la información.
57. El Servicio Central de Protección de Información Clasificada de cada Departamento Ministerial y los Servicios Generales de Protección de Información Clasificada de los Ejércitos, serán responsables de mantener, dentro de su ámbito:

    a) El Registro Centralizado de Informaciones Clasificadas.
    b) El Registro de las Directivas de Clasificación, y
    c) El Registro de las Diligencias de Clasificación.

58. La norma "NS/04 Seguridad de la Información", de la Autoridad Delegada para la Seguridad de la Información Clasificada contiene una descripción completa del Sistema de Registro y de su organización en España.7

59. Estos registros podrán ser consultados por los órganos subordinados o dependientes, para ser utilizados como criterio de clasificación.

60. Toda información registrable que se marque como clasificada, sólo adquirirá dicho carácter cuando esté correctamente anotada en un registro, para su distribución posterior.

61. El Jefe de cada Servicio de Protección es responsable de verificar que la información a registrar corresponde a algunos de los criterios o elementos contenidos en una Directiva de Clasificación o en una Diligencia de Clasificación. Si no fuera así, deberá realizarse una Propuesta de Clasificación para su posterior elevación a la Autoridad de Clasificación que corresponda.

8.6 MARCAS DE CLASIFICACIÓN

62. Los grados de clasificación estampillados sobre un determinado material clasificado, se denominan **Marcas de Clasificación**. La forma de realizar el estampillado será conforme a la normativa específica que lo regule. Como norma general, en los documentos, la marca de clasificación figurará en el encabezamiento y en el pie de cada página, diapositiva, gráfico o elemento que conforme dicho documento.

63. Una marca de clasificación consta normalmente de diferentes elementos, siendo las principales las que se indican a continuación, aunque no siempre están explícitamente presentes, salvo el grado, que es obligatorio.

64. Dichos elementos son:

Elementos de la marca	Características
TIPO	Es el ámbito de origen al que pertenece la información, es decir, la Organización o Estado propietario de la Información Clasificada. Por ejemplo: NATO, UE, NACIONAL (esta última suele ir implícita en el GRADO, por tener un idioma o nombres específicos).
GRADO	La clasificación de seguridad de la información. Por ejemplo, RESERVADO.
ESPECIALIDAD	Determinadas informaciones pertenecen a ámbitos más concretos que exigen una especial preparación y control más exhaustivo. Por ejemplo: ATOMAL, CRIPTO.

65. La documentación clasificada elaborada por Organizaciones Internacionales o proporcionada a éstas por los Estados miembro de las mismas, debe mantenerse, en lo posible, en los idiomas y formatos oficiales de las mismas. Las marcas de clasificación deben conservarse en su formato e idioma originales.

[7] Toda la documentación relativa a esas materias puede encontrarse en http://www.cni.es/es/ons/documentacion/normativa/

66. Las informaciones, asuntos y materias clasificadas por tratados o acuerdos internacionales válidamente celebrados por España e incorporados a su ordenamiento interno, así como por organizaciones internacionales aliadas o por potencias aliadas, que confieran igual grado de protección a los que son objeto de clasificación por parte española, recibirán una clasificación equivalente al de la información original.

9. PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

9.1 RESPONSABILIDAD DE LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

67. El <<ORGANISMO>> será responsable de proteger la Información Clasificada que trate, de conformidad con la legislación vigente y su propia normativa interna.

68. Cuando las unidades administrativas del <<ORGANISMO>> generen o introduzcan en las estructuras tecnológicas, redes o sistemas de información del <<ORGANISMO>> Información Clasificada que muestre una marca nacional de clasificación de seguridad, la <<U/OC>> será responsable de adoptar las medidas de protección correspondientes, con arreglo a lo exigido en el ordenamiento jurídico vigente.

69. Un volumen importante de Información Clasificada o un conjunto de la misma podrán justificar un grado de protección que se corresponda con una clasificación superior.

9.2 GESTIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN

70. La <<U/OC>> se asegurará de que la Información Clasificada tratada por el <<ORGANISMO>> se clasifique y marque adecuadamente.

71. Además de lo anterior, deberá articularse un procedimiento **de revisión periódica de la clasificación de la información**, de modo que solo conserve su grado de clasificación mientras sea necesario.

72. No se podrá rebajar el grado de clasificación de la información, ni desclasificarla, ni modificar o suprimir su categoría o las marcas a que nos hemos referido antes, sin el consentimiento previo por escrito del Responsable de la Información.8

9.3 GESTIÓN DEL RIESGO DE SEGURIDAD

73. La gestión de los riesgos respecto del tratamiento de la Información Clasificada llevado a cabo por el <<ORGANISMO>> adoptará la forma de un proceso, que tendrá por objetivo determinar los riesgos de seguridad conocidos y definir las medidas de seguridad para reducir dichos riesgos a un nivel aceptable, de conformidad con los principios básicos y requisitos mínimos establecidos en el ordenamiento jurídico vigente y, cuando proceda y resulte de aplicación, con el ENS, y adecuar tales medidas al concepto de defensa en profundidad definido en el Anexo VIII. La eficacia de dichas medidas será evaluada periódicamente.

74. Las medidas de seguridad para proteger la Información Clasificada tratada por el <<ORGANISMO>>, a lo largo de su ciclo de vida, serán acordes con su clasificación de

[8] O del órgano/organismo originador, en su caso.

seguridad, la forma y el volumen de la información, la ubicación y construcción de la instalación en el que se conserve, y la amenaza de actividades maliciosas o delictivas, evaluadas localmente, en particular el espionaje, el sabotaje y el terrorismo.

75. Los planes de contingencia tendrán en cuenta la necesidad de proteger la Información Clasificada tratada por el <<ORGANISMO>> en situaciones de emergencia, con el fin de impedir el acceso o la revelación no autorizados y la pérdida de integridad o disponibilidad.

76. En los planes de continuidad de la actividad se incluirán medidas preventivas y de recuperación para reducir al máximo las repercusiones de fallos o incidentes graves en el manejo y almacenamiento de la Información Clasificada.

9.4 SEGURIDAD LIGADA AL PERSONAL

77. Por "seguridad ligada al personal" se entenderá la aplicación de medidas que garanticen que el acceso a la Información Clasificada tratada por el <<ORGANISMO>> se concede únicamente a personas que:

- Tengan "Necesidad de Conocer",
- Hayan sido habilitadas para el grado de clasificación correspondiente, en su caso, y
- Hayan sido instruidas sobre sus responsabilidades.

78. Los procedimientos de Habilitación Personal de Seguridad (HPS) estarán concebidos para determinar si una persona puede ser autorizada para acceder a la Información Clasificada tratada por el <<ORGANISMO>>, teniendo en cuenta sus características personales.9

79. Todas las personas del <<ORGANISMO>>, internas o externas, cuyas funciones puedan requerir el acceso a Información Clasificada como CONFIDENCIAL o superior deberán haber sido habilitadas para el grado correspondiente antes de poder acceder a dicha información. Un ejemplo de procedimiento de Habilitación Personal de Seguridad para empleados públicos se muestra en el Anexo II.

80. El personal del <<ORGANISMO>> cuyas funciones puedan requerir el acceso a Información Clasificada como CONFIDENCIAL o superior, antes de poder acceder a dicha información, deberá haber sido habilitado para el grado correspondiente o haber sido debidamente autorizado en virtud de sus funciones, de conformidad con el ordenamiento jurídico vigente.

81. Antes de acceder a Información Clasificada tratada por el <<ORGANISMO>>, y de forma periódica, todas las personas deberán ser instruidas sobre sus responsabilidades en materia de protección de tal tipo de información, conforme a lo dispuesto en el presente Procedimiento, y aceptar dichas responsabilidades.

9.5 SEGURIDAD FÍSICA

[9] El procedimiento de Habilitación Personal de Seguridad se encuentra recogido en la norma "NS/02 Seguridad en el Personal – Habilitación de Seguridad del Personal", de la Autoridad Delegada para la Seguridad de la Información Clasificada.

82. Por "seguridad física" se entenderá la aplicación de medidas de protección física y técnica para impedir el acceso no autorizado a la Información Clasificada tratada por el <<ORGANISMO>>.

83. Las medidas de seguridad física estarán concebidas para:

    - Impedir la entrada, subrepticia o por la fuerza, de intrusos.
    - Disuadir, impedir y descubrir actividades no autorizadas.
    - Segregar al personal en lo que respecta al acceso a Información Clasificada, según el principio de "Necesidad de Conocer".

84. Estas medidas se determinarán a partir de un proceso de gestión del riesgo.

85. Se establecerán medidas de seguridad física en todos los locales, edificios, oficinas, salas y demás zonas en que se trate o almacene Información Clasificada, incluidas las zonas que alberguen los Sistemas de Información usados por el <<ORGANISMO>>.

86. Las zonas en que se almacene Información Clasificada de grado CONFIDENCIAL o superior se establecerán como **Zonas de Acceso Restringido**, de conformidad con Anexo III de este Procedimiento, y serán aprobadas por la Autoridad Nacional de Seguridad (ANS)10, a propuesta de la <<U/OC>> de seguridad del <<ORGANISMO>>.

87. Para la protección de Información Clasificada tratada por el <<ORGANISMO>> de grado CONFIDENCIAL o superior sólo podrán emplearse equipos o dispositivos aprobados.

9.6 CONTROL DE LA INFORMACIÓN CLASIFICADA

88. Por "control de la Información Clasificada" se entenderá la aplicación de medidas administrativas de control de la Información Clasificada tratada por el <<ORGANISMO>> a lo largo de su ciclo de vida, que contribuyan a disuadir, descubrir y subsanar cualquier acto deliberado o accidental que pueda comprometer o suponer la pérdida de dicha información. Estas medidas se refieren, en particular, a la producción, registro, copia, traducción, traslado y destrucción de la Información Clasificada tratada por el <<ORGANISMO>>.

89. La Información Clasificada de grado CONFIDENCIAL o superior se inscribirá en un Registro para fines de seguridad antes de ser distribuida y al ser recibida. La ANS establecerá a tal fin un sistema de registro. La Información Clasificada de grado SECRETO se inscribirá en registros especiales.

90. Los servicios y locales en los que se maneje o almacene Información Clasificada tratada por el <<ORGANISMO>> serán inspeccionados periódicamente por la ANS.

91. La transmisión de la Información Clasificada tratada por el <<ORGANISMO>> entre distintos servicios y/o locales, fuera de las zonas físicamente protegidas, se llevará a cabo del siguiente modo:

[10] La Autoridad Nacional de Seguridad de España es la Oficina Nacional de Seguridad (ONS), que se crea en 1983, dentro del servicio de inteligencia, como órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relativos con relación a la protección de la Información Clasificada. La ONS tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España (artículo 4 f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).

a) Como norma general, la Información Clasificada se transmitirá por medios electrónicos que estén protegidos con productos criptológicos aprobados, de conformidad con lo dispuesto en el epígrafe siguiente.
b) En caso de no utilizarse los medios contemplados en la letra a) anterior, la Información Clasificada se transportará por cualquiera de los siguientes medios:

i) medios electrónicos (por ejemplo, llaves USB, discos compactos o discos duros) que estén protegidos con productos criptológicos aprobados, de conformidad con lo dispuesto en el epígrafe siguiente, o
ii) en los restantes casos, según las prescripciones de la ANS y de acuerdo con las pertinentes medidas de protección establecidas en el Anexo IV de este Procedimiento.

9.7 PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA TRATADA EN LOS SISTEMAS DE INFORMACIÓN DEL <<ORGANISMO>>

92. Se entenderá por "Seguridad de la Información", en relación con los sistemas de información del <<ORGANISMO>>, la confianza que se tiene en que esos sistemas protejan la información que manejan y funcionen como es necesario que lo hagan, cuando así se precise, bajo el control de sus legítimos usuarios. Una Seguridad de la Información efectiva ha de garantizar unos niveles apropiados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad. La Seguridad de la Información se basará en un proceso de gestión del riesgo.

93. Para este Procedimiento, por "Sistema de Información" se entenderá el sistema que permite manejar información en formato electrónico. Un Sistema de Información abarca todos los medios necesarios para su funcionamiento, incluyendo la infraestructura, la organización y los recursos humanos e información.

94. El presente Procedimiento se aplicará a los Sistemas de Información del <<ORGANISMO>> que manejen Información Clasificada. En todo caso, los Sistemas de Información manejarán dicha Información Clasificada de conformidad con el concepto de "Seguridad de la Información" descrito.

95. Todos los Sistemas de Información serán objeto de un proceso de acreditación. La acreditación tendrá por objeto obtener garantías de que se han aplicado todas las medidas de seguridad oportunas y se ha logrado un grado de protección suficiente de la Información Clasificada tratada por el <<ORGANISMO>>, de conformidad con el presente Procedimiento. La declaración de acreditación determinará el grado máximo de clasificación de la información que pueda manejarse en un Sistema de Información concreto, y sus requisitos.

96. Los Sistemas de Información que manejen Información Clasificada de grado CONFIDENCIAL o superior deberán estar protegidos de tal manera que la información no pueda verse comprometida como consecuencia de emanaciones electromagnéticas no intencionadas ("medidas de seguridad TEMPEST").

97. Cuando la protección de la Información Clasificada tratada por el <<ORGANISMO>> se realice mediante productos criptológicos, dichos productos se aprobarán del siguiente modo:

a) La confidencialidad de la Información Clasificada de grado RESERVADO o superior deberá protegerse mediante productos criptológicos aprobados en primea instancia por el Consejo de Europa, en su calidad de Autoridad de Certificación Criptológica (ACC), por recomendación del Comité de Seguridad.
b) La confidencialidad de la Información Clasificada de grado CONFIDENCIAL o DIFUSIÓN LIMITADA deberá protegerse mediante productos criptológicos aprobados, en primera instancia, por el Secretario General del Consejo de Europa (en lo sucesivo, el "Secretario General"), en su calidad de ACC, por recomendación del Comité de Seguridad.

98. No obstante lo dispuesto en la letra b), dentro de los sistemas españoles, la confidencialidad de la Información Clasificada de grado CONFIDENCIAL o DIFUSIÓN LIMITADA podrá protegerse mediante productos criptológicos aprobados por la ANS.

99. Durante la transmisión de la Información Clasificada tratada por el <<ORGANISMO>> mediante medios electrónicos, se emplearán productos criptológicos aprobados. Sin perjuicio de este requisito, se podrán aplicar procedimientos específicos en circunstancias urgentes o en configuraciones técnicas específicas, según se indica en el Anexo V.

100. En virtud de lo dispuesto en la Decisión 2011/292/UE, de 31 de marzo, sobre normas de seguridad para la protección de la información clasificada de la UE, las autoridades competentes de la Secretaría General del Consejo de la UE y de los Estados miembros designarán, respectivamente, las siguientes funciones de Seguridad de la Información:

a) Una Autoridad de Garantía de la Información (AGI).
b) Una Autoridad TEMPEST.
c) Una Autoridad de Certificación Criptológica (ACC).
d) Una Autoridad de Distribución Criptológica (ADC).

101. Análogamente, para cada sistema, las autoridades competentes de la Secretaría General del Consejo de la UE y de los Estados miembros, respectivamente, designarán:

a) Una Autoridad de Acreditación de Seguridad (AAS).
b) Una Autoridad Operacional de Garantía de la Información (AOGI).

9.8 SEGURIDAD INDUSTRIAL

102. Por "Seguridad Industrial" se entenderá la aplicación de medidas encaminadas a garantizar la protección de la Información Clasificada tratada por los contratistas o subcontratistas durante las negociaciones precontractuales y durante la vigencia de los Contratos Clasificados. Estos contratos no podrán suponer el acceso a Información Clasificada de grado SECRETO.

103. La Secretaría General del Consejo de la UE podrá encomendar, mediante contrato, a sociedades industriales u otro tipo de entidades registradas en un Estado miembro o en un tercer Estado que haya celebrado un acuerdo o un acuerdo administrativo de conformidad con el artículo 12 de la Decisión 2011/292/UE, el desempeño de funciones que conlleven el acceso a Información Clasificada o su manejo o almacenamiento.

104. Cuando actúe como órgano de contratación, la Secretaría General del Consejo de la UE se asegurará, al adjudicar contratos clasificados a sociedades industriales u otro tipo de

entidades, de que se cumplan las normas mínimas sobre seguridad industrial que establece la Decisión antedicha y se indican en el contrato.

105. La ANS española velará, de acuerdo con el ordenamiento jurídico vigente en cada momento, para que los contratistas y subcontratistas registrados en España tomen todas las medidas adecuadas para proteger la Información Clasificada durante las negociaciones precontractuales y durante la ejecución de un Contrato Clasificado.

106. Asimismo, es responsabilidad de la ANS, de conformidad con el ordenamiento jurídico vigente, que los contratistas y subcontratistas registrados en España que participen en contratos o subcontratos clasificados que requieran el acceso a Información Clasificada de grado CONFIDENCIAL o RESERVADO en sus establecimientos, ya sea en la ejecución de dichos contratos o durante la fase precontractual, estén en posesión de una habilitación de seguridad de establecimiento del grado de clasificación requerido.

107. La ANS concederá una habilitación personal de seguridad (HPS), de conformidad con el ordenamiento jurídico y las normas mínimas de seguridad establecidas en el Anexo II, al personal del contratista o subcontratista que deba tener acceso a Información Clasificada de grado CONFIDENCIAL o RESERVADO para ejecutar un contrato clasificado.

9.9 INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

108. Cuando el Consejo de Europa determine que existe la necesidad de intercambiar Información Clasificada con un tercer Estado o una organización internacional, se establecerá un marco adecuado para ello.

109. Con el fin de establecer dicho marco y definir normas de protección recíproca de la Información Clasificada que se intercambie:

a) El Consejo de Europa celebrará acuerdos sobre procedimientos de seguridad para la protección e intercambio de Información Clasificada (en lo sucesivo, "Acuerdos para la Seguridad de la Información"), o
b) El Secretario General del Consejo podrá celebrar acuerdos administrativos a tal efecto de conformidad con el Anexo VII, si la Información Clasificada que ha de comunicarse no supera, por lo general, el grado de clasificación DIFUSIÓN LIMITADA.

110. Los acuerdos de seguridad de la información o los acuerdos administrativos a que se refiere el párrafo anterior contendrán disposiciones que garanticen que los terceros países o las organizaciones internacionales que reciban Información Clasificada protegerán dicha información de manera acorde con su grado de clasificación y conforme a normas mínimas que no sean menos estrictas que las que establece la Decisión 2011/292/UE.

111. La decisión de ceder Información Clasificada producida en el Consejo de Europa a un tercer Estado u organización internacional será adoptada por el propio Consejo, atendiendo a las circunstancias de cada caso, en función de la naturaleza y el contenido de la información, de la "Necesidad de conocer" del destinatario y de la utilidad que pueda tener para la UE. Si el originador de la Información Clasificada que se desea ceder no es el Consejo, la Secretaría General del Consejo de la UE deberá recabar el consentimiento previo por escrito del originador antes de comunicarla. En caso de que no sea posible determinar el originador, el Consejo asumirá la responsabilidad de aquel.

112. Se organizarán visitas de evaluación, a fin de verificar la eficacia de las medidas de seguridad establecidas en el tercer país o en la organización internacional de que se trate para proteger la Información Clasificada proporcionada o intercambiada.

9.10 FALLOS DE SEGURIDAD Y COMPROMISO DE LA INFORMACIÓN CLASIFICADA

113. Se produce un "compromiso" de la Información Clasificada cuando, como consecuencia de un fallo de seguridad, dicha información se pone total o parcialmente en conocimiento de personas no autorizadas.

114. Todo fallo o posible fallo de seguridad deberá comunicarse inmediatamente a la <<U/OC>> de seguridad competente del <<ORGANISMO>>, que dará cuenta a la ANS.

115. Cuando se tenga conocimiento o sospechas fundadas de que una Información Clasificada se ha visto comprometida o se ha perdido, la <<U/OC>> de seguridad competente del <<ORGANISMO>> tomará todas las medidas oportunas, de conformidad con el ordenamiento jurídico vigente, para:

a) Informar al órgano/organismo originador (o Responsable de la Información) de la información.
b) Asegurarse de que el personal que investiga el caso no esté directamente implicado en el fallo de seguridad.
c) Evaluar el posible perjuicio causado a los intereses de España, de la UE o de sus Estados miembros.
d) Tomar medidas adecuadas a fin de impedir que se repitan esos hechos, y
e) Notificar a la ANS las medidas adoptadas.

116. La persona que sea responsable de un fallo de las normas de seguridad establecidas en el presente Procedimiento podrá ser objeto de medidas disciplinarias de conformidad con la normativa aplicable. La persona que sea responsable de un compromiso o pérdida de Información Clasificada podrá ser objeto de medidas disciplinarias o de una acción judicial, de conformidad con el ordenamiento jurídico vigente.

9.11 RESPONSABILIDAD DE LA APLICACIÓN DE LA DECISIÓN 2011/292/UE

117. El Consejo de Europa tomará todas las medidas necesarias para garantizar la coherencia general de la aplicación de la Decisión 2011/292/UE, de la que trae causa el presente Procedimiento.

118. El Secretario General del Consejo de la UE tomará todas las medidas necesarias para garantizar que, cuando manejen o almacenen Información Clasificada o cualquier otra clase de Información Clasificada, tanto los funcionarios y demás agentes de la Secretaría General del Consejo de la UE como el personal destinado en comisión de servicio en la Secretaría General del Consejo de la UE y los contratistas externos de esta apliquen la presente Decisión en los locales empleados por el Consejo y dentro de la Secretaría General del Consejo de la UE, incluidas las oficinas de enlace situadas en terceros Estados.

119. Los Estados miembros adoptarán, de conformidad con sus disposiciones legales y reglamentarias nacionales, todas las medidas adecuadas para garantizar que, cuando se maneje o almacene Información Clasificada, se respete la Decisión 2011/292/UE por:

a) El personal de las Representaciones Permanentes de los Estados miembros ante la Unión Europea y por los miembros de las Delegaciones nacionales que asistan a reuniones del Consejo de la UE o de sus órganos preparatorios o que participen en otras actividades del Consejo.
b) El resto del personal de las administraciones nacionales de los Estados miembros, incluido el personal destinado en ellas en comisión de servicio, con independencia de que ejerzan sus funciones en el territorio de los Estados miembros o en el extranjero.
c) Las demás personas de los Estados miembros que, por sus funciones, estén debidamente autorizadas para acceder a Información Clasificada, y
d) Los contratistas de los Estados miembros, tanto en el territorio de los Estados miembros como en el extranjero.

9.12 ORGANIZACIÓN DE LA SEGURIDAD EN EL CONSEJO DE LA UE

120. En el marco de su función de garantizar la coherencia general en la aplicación de la Decisión 2011/292/UE, el Consejo de la UE aprobará:

a) Los acuerdos a que se refiere su artículo 12, apartado 2, letra a).
b) Las decisiones por las que se autorice la cesión de Información Clasificada a terceros Estados y organizaciones internacionales.
c) Un programa anual de inspecciones, propuesto por el Secretario General por recomendación del Comité de Seguridad, para inspeccionar los servicios y locales de los Estados miembros y de las agencias y órganos de la UE creados en virtud del título V, capítulo 2, del TUE, así como de Europol y Eurojust, y efectuar visitas de evaluación a terceros Estados y organizaciones internacionales, con el fin de verificar la eficacia de las medidas establecidas para proteger la Información Clasificada, y
d) Las políticas de seguridad a que se refiere su artículo 6, apartado 1.

121. El Secretario General será la autoridad de seguridad de la Secretaría General del Consejo de la UE. En calidad de tal, el Secretario General:

a) Aplicará la política de seguridad del Consejo y la revisará regularmente.
b) Establecerá una coordinación con las ANS de los Estados miembros para todas las cuestiones de seguridad relacionadas con la protección de Información Clasificada pertinente para las actividades del Consejo.
c) De conformidad con su artículo 7, apartado 3, concederá la HPS de la UE para el acceso a la Información Clasificada a los funcionarios y demás agentes de la Secretaría General del Consejo de la UE antes de que tengan acceso a Información Clasificada de grado CONFIDENCIAL o superior.
d) Cuando proceda, ordenará que se investigue toda situación real o supuesta de comprometimiento o pérdida de Información Clasificada que haya estado en posesión del Consejo o que haya originado este, y pedirá a las autoridades de seguridad competentes que le ayuden en dichas investigaciones.
e) Realizará inspecciones periódicas de las medidas de seguridad adoptadas para la protección de la Información Clasificada en las instalaciones de la Secretaría General del Consejo de la UE.
f) Realizará inspecciones periódicas de las medidas de seguridad adoptadas para la protección de la Información Clasificada en las agencias y órganos de la UE creados

en virtud del título V, capítulo 2, del Tratado de la UE, Europol, Eurojust, así como en las operaciones de gestión de crisis establecidas en virtud del título V, capítulo 2, del Tratado de la UE, y las adoptadas por los representantes especiales de la UE (REUE) y los miembros de sus equipos.

g) Realizará, junto con las ANS interesadas y de acuerdo con ellas, inspecciones periódicas de las medidas de seguridad adoptadas para la protección de la Información Clasificada en los servicios e instalaciones de los Estados miembros.
h) Coordinará las medidas de seguridad con las autoridades competentes de los Estados miembros que sean responsables de la protección de la Información Clasificada y, según proceda, con terceros Estados u organizaciones internacionales, en particular en lo tocante a la naturaleza de las amenazas para la seguridad de la Información Clasificada y a los medios para protegerse de ellas.
i) Celebrará los acuerdos administrativos a que se refiere su artículo 12, apartado 2, letra b), y
j) Realizará visitas de evaluación, una inicial y otras periódicas posteriormente, a los terceros Estados u organizaciones internacionales, a fin de verificar la eficacia de las medidas adoptadas para la protección de la Información Clasificada que se les haya suministrado o que se haya intercambiado con ellos.

122. La Oficina de Seguridad de la Secretaría General del Consejo de la UE se pondrá a disposición del Secretario General para prestarle ayuda en el ejercicio de estas funciones.

123. Para la aplicación de lo dispuesto en el artículo 14, apartado 3 de la Decisión 2011/292/UE, los Estados miembros:

a) Designarán una ANS responsable de los acuerdos de seguridad para la protección de la Información Clasificada, con el fin de garantizar que:

i) la Información Clasificada que esté en posesión de cualquier departamento, órgano u organismo nacional, de carácter público o privado, en el territorio nacional o en el extranjero, esté protegida de conformidad con la presente Decisión,
ii) se inspeccione periódicamente el cumplimiento de las medidas de seguridad establecidas para la protección de la Información Clasificada,
iii) toda persona empleada en una administración nacional o por un contratista a la que se pueda conceder acceso a Información Clasificada de grado CONFIDENCIAL o superior haya sido debidamente habilitada o debidamente autorizada por otros medios en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales,
iv) se elaboren los programas de seguridad que se consideren necesarios para minimizar el riesgo de que la Información Clasificada se vea comprometida o se pierda,
v) para todas las cuestiones de seguridad relacionadas con la protección de la Información Clasificada, exista una coordinación con las demás autoridades nacionales competentes, incluidas aquellas a los que se refiere la presente Decisión, y
vi) se dé respuesta a las solicitudes adecuadas de habilitación de seguridad remitidas por las agencias y órganos creados en virtud del título V, capítulo 2, del Tratado de la UE, Europol, Eurojust, así como en las operaciones de gestión de crisis establecidas en virtud del título V, capítulo 2, del Tratado de la UE y por los REUE y sus equipos.
La lista de las ANS figura en el apéndice C de la precitada Decisión que, en lo referente a España, señala:

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

b) Se asegurarán de que sus autoridades competentes informen y asesoren a sus respectivos gobiernos y, a través de estos, al Consejo, acerca de la naturaleza de las amenazas que pesan sobre la seguridad de la Información Clasificada y sobre los medios para protegerse de ellas.

9.13 COMITÉ DE SEGURIDAD DE LA UE

124. La Decisión 2011/292/UE crea un Comité de Seguridad de la UE cuyas funciones consistirán en examinar y evaluar las cuestiones de seguridad incluidas en el ámbito de aplicación de tal Decisión, haciendo recomendaciones al Consejo cuando proceda.

125. El Comité de Seguridad estará integrado por representantes de las ANS de los Estados miembros, asistiendo a sus reuniones un representante de la Comisión y del Servicio Europeo de Acción Exterior. El Comité de Seguridad estará presidido por el Secretario General o por la persona en quien este delegue. Se reunirá siguiendo instrucciones del Consejo o a instancias del Secretario General o de una ANS.

126. Se podrá invitar a representantes de las agencias y órganos de la UE creados en virtud del título V, capítulo 2, del Tratado de la UE, así como de Europol y Eurojust, a asistir a las reuniones cuando se debatan cuestiones que los afecten.

127. El Comité de Seguridad organizará sus actividades de manera que pueda formular recomendaciones sobre aspectos específicos de la seguridad. Creará una subsección de expertos en cuestiones relativas a la Seguridad de la Información, así como otras subsecciones de expertos, si fuera necesario. Elaborará los mandatos para dichas subsecciones y recibirá los informes que estas realicen sobre sus actividades, entre los que podrán figurar, si se considera oportuno, recomendaciones para el Consejo.

ANEXO I

GRADOS DE CLASIFICACIÓN

1. MATERIAS CLASIFICADAS

1.1. GRADO SECRETO

La clasificación de **SECRETO** se aplicará a la información que precise del más alto grado de protección, cuando su revelación no autorizada o utilización indebida pudiera dar lugar a una amenaza o perjuicio extremadamente grave para los intereses de España, en los siguientes ámbitos:

a) La soberanía e integridad territorial.
b) El orden constitucional y la seguridad del Estado.
c) El orden público y la vida de los ciudadanos.
d) La capacidad de combate o la seguridad de las Fuerzas Armadas de España o de sus aliados.
e) La efectividad o la seguridad de operaciones de excepcional valor de los servicios de inteligencia de España o de sus aliados.
f) Las relaciones diplomáticas de España o situaciones de tensión internacional.
g) Cualquier otro cuya salvaguarda requiera de la más alta protección.
h) Cualquiera que así sea declarada por ley.

1.2. GRADO RESERVADO

La clasificación de **RESERVADO** se aplicará a la información que precise de un alto grado de protección cuando, su revelación no autorizada o utilización indebida pudiera dar lugar a una amenaza o perjuicio grave para los intereses de España, en los siguientes ámbitos:

a) El orden constitucional y la seguridad del Estado.
b) El orden público y la seguridad de los ciudadanos.
c) La capacidad de combate o la seguridad de las Fuerzas Armadas de España o de sus aliados.
d) La efectividad o la seguridad de operaciones de los servicios de inteligencia de España o de sus aliados.
e) Las relaciones diplomáticas de España o situaciones de tensión internacional.
f) Los intereses económicos o industriales de carácter estratégico.
g) Cualquier otro cuya salvaguarda requiera de un alto grado de protección.
h) Cualquiera que así sea declarada por ley.

2. MATERIAS DE RESERVA INTERNA

2.1. GRADO CONFIDENCIAL

La clasificación de CONFIDENCIAL se aplicará a la información cuya revelación no autorizada o utilización indebida pudiera causar una amenaza o perjuicio para los intereses de España en los siguientes ámbitos:

a) El efectivo desarrollo de las políticas del Estado o el funcionamiento del sector público.
b) Negociaciones políticas o comerciales de España frente a otros Estados.
c) Los intereses económicos o industriales.
d) Funcionamiento de los servicios públicos.
e) Dificultar la investigación o facilitar la comisión de delitos.
f) Cualquier otro que pueda causar una amenaza o perjuicio para los intereses de España.

2.2. GRADO DIFUSIÓN LIMITADA

La clasificación de **DIFUSIÓN LIMITADA** se aplicará a la información cuya revelación no autorizada o utilización indebida pudiera ser contraria a los intereses de España en cualquiera de los ámbitos relacionados en los apartados anteriores.

ANEXO II

SEGURIDAD LIGADA AL PERSONAL

1. INTRODUCCIÓN

El presente Anexo define los criterios que determinan si una persona, teniendo en cuenta sus características personales, esencialmente: lealtad, honradez y confiabilidad[11], puede ser autorizada para acceder a Información Clasificada tratada por el <<ORGANISMO>> de que se trate, y los procedimientos administrativos y de investigación que han de seguirse a tal efecto.

A lo largo del presente Anexo, salvo cuando la distinción sea pertinente, el término "Habilitación Personal de Seguridad" se empleará indistintamente para referirse a la Habilitación Personal de Seguridad nacional (HPS nacional) y a la Habilitación Personal de Seguridad de la UE (HPS UE), tal como se definen en el Anexo VIII (Definiciones) del presente Procedimiento.

2. AUTORIZACIÓN DE ACCESO A LA INFORMACIÓN CLASIFICADA TRATADA POR EL <<ORGANISMO>>

Sólo se concederá autorización para acceder a Información Clasificada de grado CONFIDENCIAL o superior a aquella persona:

a) Cuya "Necesidad de Conocer" se haya determinado previamente,
b) A quien se haya concedido una HPS del grado correspondiente, o a quien se haya autorizado debidamente en virtud de sus funciones, de conformidad con el ordenamiento jurídico vigente, y
c) Que haya sido instruida sobre las normas y procedimientos de seguridad para la protección de la Información Clasificada tratada por el <<ORGANISMO>>, y que haya aceptado sus responsabilidades en lo que respecta a la protección de dicha información.

El <<ORGANISMO>> determinará los puestos de trabajo que, dentro de su competencia, puedan exigir el acceso a Información Clasificada de grado CONFIDENCIAL o superior y requieran por tanto una HPS del grado que corresponda.

3. REQUISITOS PARA OBTENER LA HABILITACIÓN PERSONAL DE SEGURIDAD

Una vez recibida una solicitud debidamente autorizada, corresponderá a la Autoridad Nacional de Seguridad (ANS)[12] asegurarse de que se realizan las investigaciones de seguridad

[11] Según dispone la Decisión del Consejo 2011/292/UE, de 31 de marzo, sobre las normas de seguridad para la protección de la Información Clasificada de la UE.

[12] Competencias asignadas a la Oficina Nacional de Seguridad, dependiente del Centro Nacional de Inteligencia (CNI). La Oficina Nacional de Seguridad (ONS) se crea en 1983, dentro del servicio de inteligencia, como órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relativos con relación a la protección de la Información Clasificada. La ONS tiene por misión fundamental la de velar por el

sobre aquellas personas (de nacionalidad española) que deban tener acceso a Información Clasificada de grado CONFIDENCIAL o superior. Las investigaciones se ajustarán a lo dispuesto en el ordenamiento jurídico español.

En caso de que la persona resida en el territorio de otro Estado miembro o en un tercer Estado, la ANS solicitará la colaboración de la autoridad competente del Estado de residencia, de conformidad con las disposiciones legales y reglamentarias nacionales.

Cuando lo permita el ordenamiento jurídico, la ANS podrá realizar investigaciones sobre no nacionales que deban tener acceso a Información Clasificada de grado CONFIDENCIAL o superior. Las investigaciones se ajustarán a lo dispuesto en el ordenamiento jurídico español.

Criterios para las investigaciones de seguridad

La lealtad, honradez y confiabilidad de una persona a efectos de la concesión de una HPS para acceder a Información Clasificada de grado CONFIDENCIAL o superior se determinarán mediante una investigación de seguridad. La ANS realizará una evaluación global basada en el resultado de la investigación de seguridad. Un único hallazgo negativo no constituirá necesariamente razón suficiente para denegar una HPS.

Los criterios principales que se aplicarán a este efecto incluirán, en la medida en que lo posibilite el ordenamiento jurídico, el estudio de si la persona:

a) Ha cometido o intentado cometer cualquier acto de espionaje, terrorismo, sabotaje, traición o sedición; o ha conspirado para su comisión o ha sido cómplice de su comisión.
b) Está o ha estado vinculada con organizaciones de espionaje, terrorismo, saboteadores o personas sobre las que pese una sospecha razonable de pertenecer a estos grupos, o con representantes de organizaciones o Estados extranjeros, incluidos los servicios de inteligencia extranjeros, que puedan suponer una amenaza para la seguridad de la UE o de sus Estados miembros, salvo que dicha relación haya sido autorizada en cumplimiento de una misión oficial.
c) Es o ha sido miembro de cualquier organización que persiga, por medios violentos, subversivos u ilegales, el derrocamiento del gobierno de un Estado miembro de la UE, la alteración del orden constitucional de un Estado miembro de la UE o el cambio de su forma de gobierno o de la política de su gobierno.
d) Respalda o ha respaldado a cualquier organización que responda a lo descrito en la letra c), o está estrechamente vinculado a miembros de este tipo de organizaciones.
e) Ha ocultado, deformado o falseado deliberadamente información importante, especialmente en el ámbito de la seguridad, o ha mentido deliberadamente al cumplimentar un cuestionario de seguridad personal o en el curso de una entrevista de seguridad.
f) Ha sido condenado por uno o varios delitos.
g) Tiene un historial de dependencia del alcohol, consumo de drogas ilícitas o consumo abusivo de drogas lícitas.
h) Tiene o ha tenido alguna conducta que pueda hacerlo vulnerable al chantaje u otro tipo de presiones.

cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España (artículo 4 f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).

i) Ha demostrado, de obra o de palabra, su falta de honradez, deslealtad, falta de confiabilidad o de probidad.
j) Ha infringido de manera grave o reiterada las normas de seguridad, o ha intentado realizar o ha realizado actividades no autorizadas en relación con sistemas de información y comunicaciones.
k) Puede verse sujeto a presiones (por ejemplo, por tener la nacionalidad de uno o varios países no pertenecientes a la UE o a través de familiares o allegados que puedan ser vulnerables frente a servicios de inteligencia extranjeros, grupos terroristas u otras organizaciones, o personas subversivas cuyos fines puedan amenazar la seguridad de la UE o de los Estados miembros).

Cuando proceda, y de conformidad con el ordenamiento jurídico vigente, se podrá considerar pertinente para la investigación de seguridad las circunstancias económicas o el historial médico de una persona.

Cuando proceda, y de conformidad con el ordenamiento jurídico vigente, podrán también considerarse pertinentes para la investigación de seguridad, el carácter, la conducta y las circunstancias del cónyuge, un cohabitante o un miembro cercano de la familia.

Requisitos de investigación a efectos del acceso a Información Clasificada tratada por el <<ORGANISMO>>

Primera concesión de una HPS

La HPS inicial para acceder a información de los grados **CONFIDENCIAL y RESERVADO** se basará en una investigación de seguridad que abarque un período de, al menos, los cinco últimos años, o bien desde que la persona cumplió los 18 años de edad hasta el momento presente, eligiendo el período más corto, y que incluirá los siguientes elementos:

a) Cumplimentación de un *Cuestionario Personal de Seguridad* para el grado de Información Clasificada a la que solicita tener acceso la persona investigada. Una vez cumplimentado, el cuestionario se remitirá a la ANS.
b) Comprobación de la identidad, ciudadanía o nacionalidad de la persona. Se verificará la fecha y lugar de nacimiento del solicitante y se comprobará su identidad. Se determinará asimismo su ciudadanía o nacionalidad, pasada y presente. Esta comprobación incluirá una evaluación de la posible vulnerabilidad frente a presiones de fuentes extranjeras, por ejemplo debido a su lugar de residencia anterior o a vinculaciones con el pasado, etc., y
c) Comprobación de los registros nacionales y locales. Se comprobarán los registros nacionales de seguridad y el de antecedentes penales, u otros registros similares de las administraciones públicas y de las Fuerzas y Cuerpos de Seguridad. Deberán comprobarse los registros policiales o judiciales con competencia territorial en los lugares donde haya residido o trabajado la persona investigada.

La HPS inicial para acceder a Información Clasificada de grado **SECRETO** se basará en una investigación de seguridad que abarque un período de, al menos, los diez últimos años, o bien desde que el solicitante cumplió 18 años de edad hasta el momento presente, eligiendo el período más corto. En caso de realizarse entrevistas conforme a lo previsto en la letra e) anterior, las investigaciones abarcarán un período de, al menos, los siete últimos años, o bien desde que la persona cumplió 18 años de edad hasta el momento presente, eligiendo el período más corto.

Además de los criterios indicados anteriormente, antes de conceder una HPS de grado SECRETO deberán realizarse indagaciones, en la medida en que lo permita el ordenamiento jurídico, sobre los factores que se indican a continuación. Estos factores también pueden ser pertinentes antes de conceder una HPS de grado CONFIDENCIAL o SECRETO cuando así lo exija el ordenamiento jurídico vigente.

a) Situación económica: se investigará este extremo con el fin de evaluar si es vulnerable frente a posibles presiones de procedencia extranjera o nacional por sufrir dificultades económicas graves, o con el fin de descubrir ingresos económicos inexplicables.
b) Educación: se investigará este extremo a fin de verificar los antecedentes académicos de la persona en escuelas, universidades y otros centros de enseñanza a los que haya asistido desde que haya cumplido 18 años de edad o durante el período que estime conveniente la autoridad que efectúa la investigación.
c) Empleos: se investigará el trabajo actual y los anteriores, consultando registros e informes sobre rendimiento o eficiencia, y la opinión de los empleadores o superiores jerárquicos.
d) Servicio militar: cuando proceda, se verificará la prestación del servicio militar de la persona y las circunstancias de su baja, y
e) Entrevistas: siempre y cuando lo permita y prevea el ordenamiento jurídico, se mantendrán una o varias entrevistas con la persona. También se entrevistará a otras personas que estén en condiciones de hacer una valoración imparcial de los antecedentes, las actividades, la lealtad, honradez y confiabilidad del interesado. Si el procedimiento pudiera implicar la solicitud de garantes al sujeto de la investigación, se entrevistará a las personas que hayan aportado referencias, salvo que existan motivos justificados para no hacerlo.

Cuando sea necesario, y de conformidad con el ordenamiento jurídico vigente, podrán realizarse investigaciones adicionales con el fin de profundizar en toda la información pertinente de que se disponga sobre una persona, y para confirmar o desmentir la información desfavorable.

Renovación de las HPS

Tras la concesión inicial de una HPS, y siempre que la persona haya prestado servicio de forma ininterrumpida en algún órgano u organismo de las AA.PP. españolas o en las de la UE y siga necesitando acceder a Información Clasificada, la HPS se revisará con vistas a su renovación por períodos no superiores a cinco años para las habilitaciones SECRETO, y a diez años para las habilitaciones RESERVADO y CONFIDENCIAL, contados a partir de la fecha de notificación del resultado de la última investigación de seguridad que haya servido de base para dichas habilitaciones. Todas las investigaciones de seguridad a efectos de la renovación de una HPS abarcarán el período transcurrido desde la anterior investigación de seguridad.

Para la renovación de las HPS se investigarán los factores señalados en los puntos anteriores.

Las solicitudes de renovación se cursarán con la debida antelación, teniendo en cuenta el tiempo necesario para efectuar las investigaciones de seguridad. No obstante, si la ANS hubiese recibido la oportuna solicitud de renovación y el correspondiente *Cuestionario Personal de Seguridad* antes de que caduque la habilitación de seguridad y no hubiese finalizado la investigación de seguridad requerida, la ANS podrá, si así lo permite el ordenamiento jurídico, prorrogar la validez de la HPS vigente por un plazo no superior a 12

meses. Si al término de este período de 12 meses la investigación de seguridad no hubiese concluido aún, la persona solo podrá desempeñar funciones que no requieran una HPS.

Registros de las HPS

España, como Estado miembro de la UE destinatario de la Decisión 2011/292/UE, de 31 de marzo, sobre normas de seguridad para la protección de la Información Clasificada de la UE, llevará registro de las HPS nacionales que hayan concedido para acceder a Información Clasificada tratada por los diferentes organismos de las AA.PP. españolas. Este registro indicará, como mínimo, el grado de la Información Clasificada al que la persona puede tener acceso (CONFIDENCIAL o superior), la fecha de concesión de la habilitación y su período de validez.[13]

La ANS competente podrá expedir un **Certificado de Habilitación Personal de Seguridad** (CHPS) que acredite a qué grado de Información Clasificada puede tener acceso la persona (CONFIDENCIAL o superior), la fecha de validez de la HPS para acceder a Información Clasificada y la fecha de caducidad del propio certificado.

4. FORMACIÓN Y SENSIBILIZACIÓN EN MATERIA DE SEGURIDAD

Todas las personas a las que se haya otorgado una HPS declararán por escrito que han entendido sus obligaciones respecto a la protección de la Información Clasificada y las consecuencias derivadas de un posible compromiso de esta información. La ANS –y cada <<ORGANISMO>>, respecto de sus propias declaraciones- llevará un registro de estas declaraciones escritas.

El <<ORGANISMO>>, a través de su <<U/OC>> de seguridad competente lo será de sensibilizar a todas las personas que estén autorizadas para acceder a la Información Clasificada tratada por el <<ORGANISMO>> o que deban manejar este tipo de información, respecto de las amenazas a la seguridad. Dichas personas deberán dar cuenta inmediatamente a la <<U/OC>> competente del <<ORGANISMO>> de cualquier actitud o actividad que consideren sospechosa o inusual.

Todas las personas que dejen de desempeñar funciones que hubieren requerido el acceso a Información Clasificada tratada por el <<ORGANISMO>> serán aleccionadas sobre su obligación de seguir protegiendo dicha información, y, en su caso, deberán reconocer tal obligación por escrito.

5. CIRCUNSTANCIAS EXCEPCIONALES

En caso de que se vaya a destinar a una persona a un puesto que requiera una HPS de un grado superior al que posea en ese momento, el nombramiento podrá efectuarse a título provisional, siempre que:

a) El superior jerárquico de la persona justifique por escrito la necesidad imperiosa de acceso a Información Clasificada de un grado superior.
b) Para el desempeño de su función, el acceso se limite a elementos concretos de Información Clasificada.
c) La persona disponga de una HPS nacional o HPS UE en vigor.

[13] Podrán existir registros a nivel de <<ORGANISMO>>, siempre que lo apruebe la ANS.

d) Se hayan iniciado los trámites para la obtención de la autorización de acceso del nivel que el puesto requiera.
e) La autoridad competente haya comprobado a su satisfacción que la persona no ha infringido de manera grave o reiterada las normas de seguridad.
f) El nombramiento de la persona haya sido aprobado por la autoridad competente, y
g) El encargado del registro hará constar la excepción, con una descripción de la información para la cual se haya autorizado el acceso.

Este procedimiento se utilizará para un único acceso a Información Clasificada del grado inmediatamente superior a aquel para el que la persona esté habilitada. En ningún caso podrá utilizarse este procedimiento de forma reiterada.

En circunstancias muy excepcionales[14], la ANS podrá autorizar, a ser posible por escrito, el acceso a información de grado CONFIDENCIAL o RESERVADO a personas que no posean la HPS exigida, siempre que dicha autorización sea imprescindible y no existan dudas razonables sobre la lealtad, honradez y confiabilidad de la persona de que se trate. Dicha autorización se registrará, junto con una descripción de la información para la cual se haya autorizado el acceso.

En el caso de la Información Clasificada de grado SECRETO, este acceso de urgencia estará limitado a los nacionales de la UE que hayan sido autorizados para acceder o bien a Información Clasificada de grado SECRETO o bien a Información Clasificada de grado RESERVADO.

Cuando el ordenamiento jurídico vigente establezca normas más estrictas en lo relativo a autorizaciones temporales, nombramientos provisionales, acceso único o acceso de urgencia a Información Clasificada, los procedimientos mencionados se estará a lo dispuesto en la regulación nacional.

6. ACCESO POTENCIAL A INFORMACIÓN CLASIFICADA

Las personas que en el desempeño de sus funciones tuvieren posibilidad de acceder a Información Clasificada de grado CONFIDENCIAL o superior deberán estar debidamente habilitadas o ir escoltadas en todo momento.

Los correos, agentes de seguridad y escoltas estarán debidamente habilitados para el grado correspondiente y/o serán investigados de forma apropiada, según el ordenamiento jurídico vigente, aleccionándoles sobre los procedimientos de seguridad para la protección de la Información Clasificada y se les instruirá acerca de sus obligaciones en materia de protección de la información que se les confíe.

[14] Tales como misiones en un medio hostil o durante períodos de incremento de la tensión internacional, cuando así lo requieran medidas de urgencia y, en particular, cuando estén en peligro vidas humanas.

ANEXO III

SEGURIDAD FÍSICA

1. INTRODUCCIÓN

El presente Anexo define los requisitos mínimos para la protección física de los locales, edificios, oficinas, salas y demás zonas donde el <<ORGANISMO>> trate, maneje o almacene Información Clasificada, incluidas las zonas que alojen Sistemas de Información.

Las medidas de seguridad física estarán concebidas para impedir el acceso no autorizado a la Información Clasificada tratada por el <<ORGANISMO>> para:

a) Garantizar que la Información Clasificada tratada por el <<ORGANISMO>> se maneje y se almacene adecuadamente.
b) Permitir la separación del personal en su acceso a Información Clasificada en función de su "Necesidad de conocer" y, en su caso, de su habilitación de seguridad.
c) Disuadir, impedir y detectar actividades no autorizadas, e
d) Impedir o retrasar la entrada subrepticia o por la fuerza de intrusos.

2. REQUISITOS Y MEDIDAS DE SEGURIDAD FÍSICA

Las medidas de seguridad física aplicables se determinarán sobre la base de una evaluación de las amenazas realizada por la ANS. Para ello, se aplicará un proceso de gestión de riesgos para proteger la Información Clasificada tratada por el <<ORGANISMO>> en sus respectivos locales, de modo que se garantice un grado de protección física acorde con el riesgo evaluado.

El proceso de gestión del riesgo tendrá en cuenta todos los factores pertinentes, en particular:

a) El grado de clasificación de la Información Clasificada tratada por el <<ORGANISMO>>.
b) La forma y volumen de la Información Clasificada tratada por el <<ORGANISMO>>, teniendo presente que grandes cantidades de Información Clasificada o su recopilación podrían requerir la aplicación de medidas de protección más estrictas.
c) El entorno y la estructura de los edificios o zonas donde se almacene Información Clasificada, y
d) La evaluación de las amenazas que tienen como objetivo la UE y sus Estados miembros como el sabotaje, el terrorismo, la subversión u otras actividades delictivas.

Al aplicar el concepto de defensa en profundidad, las ANS determinará la combinación apropiada de las medidas de seguridad física que deben aplicarse en cada caso, pudiendo incluir una o varias de las siguientes medidas:

a) Barreras perimetrales: barreras físicas para la protección de los límites exteriores de la zona concreta.
b) Sistemas de detección de intrusiones (SDI): pudiendo emplearse para aumentar el grado de seguridad que brinda la barrera perimetral o -en determinadas salas y edificios- en sustitución o como complemento del personal de seguridad.

c) Controles de acceso: pudiendo aplicarse en una instalación, en un edificio o edificios de una instalación o en zonas o salas situadas dentro de un edificio. El control puede realizarse por medios electrónicos o electromecánicos, por medio de personal de seguridad, de un recepcionista o de ambos, o por cualquier otro medio físico.
d) Personal de seguridad: puede emplearse, entre otros recursos, personal de seguridad debidamente formado y, en caso necesario, con la debida habilitación de seguridad para disuadir a posibles intrusos que pudieran perpetrar una entrada encubierta.
e) Sistemas de circuito cerrado de televisión (CCTV): estos sistemas pueden ser utilizados por el personal de seguridad para verificar incidentes y alarmas del SDI en emplazamientos de gran extensión o en el perímetro de una zona.
f) Iluminación de seguridad: la iluminación de seguridad puede emplearse para disuadir a posibles intrusos, además de proporcionar la iluminación necesaria para una vigilancia eficaz, bien directamente por parte del personal de seguridad, bien de forma indirecta a través de un CCTV, y
g) Cualquier otra medida apropiada de seguridad física destinada a disuadir o detectar entradas no autorizadas o a prevenir la pérdida o deterioro de Información Clasificada tratada por el <<ORGANISMO>>.

Podrá autorizarse a la <<U/OC>> de seguridad competente para llevar a cabo, en las entradas y las salidas, registros que disuadan de todo intento no autorizado de introducir material en los locales o edificios o de extraer de ellos Información Clasificada.

Cuando exista riesgo de que una Información Clasificada tratada por el <<ORGANISMO>> sea objeto de miradas indiscretas, incluso accidentalmente, se tomarán medidas adecuadas para contrarrestar ese riesgo.

Para nuevas instalaciones, los requisitos de seguridad física y sus especificaciones funcionales se definirán en el momento de la planificación y el diseño del mismo. Para los establecimientos ya existentes, los requisitos de seguridad física se aplicarán en la mayor medida posible.

3. EQUIPAMIENTO PARA LA PROTECCIÓN FÍSICA DE LA INFORMACION CLASIFICADA TRATADA POR EL <<ORGANISMO>>

La <<U/OC>> de seguridad competente del <<ORGANISMO>> se asegurará de que el equipamiento que se adquiera para la protección física de la Información Clasificada (armarios de seguridad, trituradoras de papel, cerraduras, sistemas electrónicos de control de acceso, sistemas de detección de intrusos, sistemas de alarma, etc.) cumpla los estándares técnicos y los requisitos mínimos aprobados.

Las especificaciones técnicas del equipamiento que vaya a emplearse para la protección física de la Información Clasificada tratada por el <<ORGANISMO>> se establecerán en directrices de seguridad que deberán ser aprobadas por el Comité de Seguridad de la UE y comunicadas por la ANS a los organismos finales.

Los sistemas de seguridad se inspeccionarán periódicamente y se realizará un mantenimiento del equipamiento con regularidad. Para las operaciones de mantenimiento se tendrá en cuenta el resultado de las inspecciones, a fin de garantizar que el citado equipamiento siga funcionando óptimamente.

La eficacia de cada medida de seguridad y del sistema de seguridad en su conjunto se reevaluará en cada inspección.

4. ZONAS FÍSICAMENTE PROTEGIDAS

Para la protección material de la Información Clasificada tratada por el <<ORGANISMO>> se establecerán dos tipos de zonas físicamente protegidas:

a) *Zonas Administrativas*, y
b) *Zonas de Acceso Restringido* (incluidas las zonas de acceso restringido protegidas por medios técnicos).

La <<U/OC>> de seguridad competente del <<ORGANISMO>> decidirá si una zona cumple los requisitos para ser designada zona administrativa, zona de acceso restringido o zona acceso restringido protegida por medios técnicos.

Para las **Zonas Administrativas**:

a) Se establecerá un perímetro visiblemente definido que permita el control de personas y, cuando sea posible, de vehículos.
b) Sólo se permitirá el acceso sin acompañamiento a las personas debidamente autorizadas por la <<U/OC>> de seguridad competente, y
c) El resto de personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.

Para las **Zonas de Acceso Restringido**:

a) Se establecerá un perímetro visiblemente definido y protegido en el que se controlen todas las entradas y salidas mediante un sistema de acreditaciones o de identificación personal.
b) Sólo se permitirá el acceso sin acompañamiento a las personas que tengan una habilitación de seguridad y una autorización específica para entrar en la zona atendiendo siempre a su "Necesidad de conocer".
c) El resto de personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.

Cuando la entrada en una zona de acceso restringido equivalga en la práctica a tener acceso directo a la Información Clasificada que se encuentre en la zona, se aplicarán, además, los siguientes controles:

a) Se indicará con claridad el máximo grado de clasificación de seguridad de la información que se encuentre en dicha zona.
b) Todos los visitantes necesitarán una autorización específica para acceder a la zona, y estarán acompañados en todo momento y debidamente habilitados, salvo que se tomen medidas para que no sea posible que accedan a la Información Clasificada tratada por el <<ORGANISMO>>.

Las zonas de acceso restringido protegidas contra escuchas serán designadas como **Zonas de Acceso Restringido protegidas por medios técnicos**. Se aplicarán los controles adicionales siguientes:

a) Estas zonas estarán equipadas con sistemas de detección de intrusos, se cerrarán con llave cuando no estén ocupadas y se vigilarán cuando estén ocupadas. Todas las llaves se controlarán de acuerdo con lo dispuesto en el epígrafe 6.
b) Todas las personas y el material que entren en estas zonas serán objeto de control.
c) Estas zonas serán objeto de inspecciones físicas o técnicas regularmente, según lo requiera la <<U/OC>> de seguridad competente. Además, también serán inspeccionadas cada vez que se haya producido o se sospeche que se ha producido una entrada no autorizada, y
d) No habrá en estas zonas ninguna línea de comunicaciones, teléfono o cualquier otro equipo de comunicaciones, ni aparatos eléctricos o electrónicos, salvo aquellos que estén expresamente autorizados individualmente.

No obstante lo dispuesto en la letra d) anterior, todos los equipos de comunicaciones y todos los aparatos eléctricos o electrónicos deberán ser examinados por la <<U/OC>> de seguridad competente antes de que puedan ser utilizados en zonas donde se estén celebrando reuniones o realizando trabajos en que se maneje Información Clasificada de grado RESERVADO o superior, así como cuando la amenaza para la Información Clasificada tratada por el <<ORGANISMO>> se considere elevada. Todo ello con el fin de garantizar que ninguna información en claro pueda transmitirse de manera involuntaria o ilícita a través de dichos equipos más allá del perímetro de la zona de acceso restringido de que se trate.

Las zonas de acceso restringido que no estén ocupadas por personal de servicio las veinticuatro horas del día se inspeccionarán, en su caso, al final de la jornada normal de trabajo y a intervalos aleatorios fuera de dicha jornada, a menos que se haya instalado en ellas un sistema de detección de intrusos.

Se podrán establecer con carácter temporal zonas de acceso restringido y zonas de acceso restringido protegidas por medios técnicos en una zona administrativa para la celebración de una reunión clasificada u otro motivo similar.

Para cada zona de acceso restringido se definirán procedimientos operativos de seguridad en los que se disponga lo siguiente:

a) El grado de la Información Clasificada que puede manejarse o almacenarse en la zona.
b) Las medidas de vigilancia y protección que hayan de aplicarse.
c) Las personas autorizadas para entrar en ella sin acompañamiento, atendiendo a su "Necesidad de Conocer" y de su habilitación de seguridad.
d) En su caso, los procedimientos aplicables a los acompañantes o a la protección de la Información Clasificada cuando se autorice la entrada de cualquier otra persona en la zona.
e) Cualquier otra medida o procedimiento pertinente.

Las cámaras acorazadas se ubicarán en zonas de acceso restringido. Los muros, suelos, techos, ventanas y puertas que puedan cerrarse con llave deberán haber sido aprobados por la <<U/OC>> de seguridad competente y ofrecer una protección equivalente a la de un contenedor de seguridad aprobado para el almacenamiento de Información Clasificada del mismo grado de clasificación.

5. MEDIDAS DE PROTECCIÓN FÍSICA PARA EL MANEJO Y ALMACENAMIENTO DE LA INFORMACIÓN CLASIFICADA TRATADA POR EL <<ORGANISMO>>

La Información Clasificada tratada por el <<ORGANISMO>> de grado DIFUSIÓN LIMITADA se podrá manejar:

a) En una Zona de Acceso Restringido.
b) En una Zona Administrativa, siempre que el acceso a la Información Clasificada esté protegido frente a personas no autorizadas, o
c) Fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la Información Clasificada de conformidad con lo establecido en el Anexo IV y se haya comprometido a cumplir las medidas supletorias establecidas en las instrucciones de seguridad definidas por la <<U(OC>> de seguridad competente para garantizar que la Información Clasificada tratada por el <<ORGANISMO>> está protegida del acceso de personas no autorizadas.

La Información Clasificada tratada por el <<ORGANISMO>> de grado **DIFUSIÓN LIMITADA** se guardará en muebles de oficina cerrados con llave, en las zonas administrativas o las zonas de acceso restringido. La Información Clasificada de dicho grado podrá almacenarse temporalmente fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor se haya comprometido a cumplir las medidas supletorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente.

La Información Clasificada tratada por el <<ORGANISMO>> de grado **CONFIDENCIAL** o **RESERVADO** se podrá manejar:

a) En una Zona de Acceso Restringido.
b) En una Zona Administrativa, siempre que se impida el acceso a la Información Clasificada a personas no autorizadas, o
c) Fuera de una zona de acceso restringido o de una zona administrativa siempre que el poseedor:

   i) transporte la Información Clasificada de conformidad con lo dispuesto en el Anexo IV,
   ii) se haya comprometido a cumplir las medidas supletorias establecidas en las instrucciones de seguridad definidas por la <<U/OC>> de seguridad competente para garantizar que el acceso a la Información Clasificada tratada por el <<ORGANISMO>> se impide a personas no autorizadas,
   iii) mantenga la Información Clasificada en todo momento bajo su control personal, y
   iv) en el caso de documentos en papel, haya notificado el hecho al registro correspondiente.

La Información Clasificada tratada por el <<ORGANISMO>> de grado CONFIDENCIAL y RESERVADO se almacenará en una zona de acceso restringido dentro de un contenedor de seguridad o una cámara acorazada.

La Información Clasificada tratada por el <<ORGANISMO>> de grado SECRETO se manejará en una Zona de Acceso Restringido, bajo una de las siguientes condiciones:

a) En un contenedor de seguridad, conforme a lo dispuesto en el epígrafe 8, con uno o varios de los controles adicionales siguientes:

   i) protección continua o verificación periódica por personal de seguridad o de servicio habilitado,
   ii) un SDI aprobado, junto con personal de seguridad para intervención en caso de incidente, o

b) En una cámara acorazada con SDI, junto con personal de seguridad para intervención en caso de incidente.

En el Anexo IV se recogen las normas para el transporte de Información Clasificada tratada por el <<ORGANISMO>> fuera de las zonas físicamente protegidas.

6. CONTROL DE LLAVES/CLAVES DE APERTURA EMPLEADAS PARA LA PROTECCIÓN DE LAINFORMACIÓN CLASIFICADA TRATADA POR EL <<ORGANISMO>>

La <<U/OC>> de seguridad competente definirá procedimientos para la gestión de las llaves/claves de apertura de las oficinas, salas, cámaras acorazadas y contenedores de seguridad. Estos procedimientos deberán evitar accesos no autorizados.

Las claves serán confiadas al menor número posible de personas que necesiten conocerlas. Las claves de los contenedores de seguridad y cámaras acorazadas en los que se almacene e Información Clasificada se modificarán:

a) Cada vez que cambie el personal que conoce la combinación.
b) Cada vez que se haya producido o se sospeche que se ha producido una situación de comprometimiento de la clave.
c) Cuando se hayan realizado operaciones de mantenimiento o reparación de una cerradura, y
d) Al menos, cada 12 meses.

ANEXO IV

CONTROL DE LA INFORMACIÓN CLASIFICADA

1. INTRODUCCIÓN

El presente Anexo establece las medidas administrativas para controlar la Información Clasificada tratada por el <<ORGANISMO>> a lo largo de su ciclo de vida, con el fin de prevenir, detectar y subsanar el comprometimiento o la pérdida -accidental o deliberada- de dicha información.

2. GESTIÓN DE LA CLASIFICACIÓN

Clasificaciones y marcas

La información se clasificará cuando requiera protección respecto de su confidencialidad.

El órgano/organismo originador de la Información Clasificada será responsable de determinar el grado de clasificación de seguridad atendiendo a las directrices de clasificación pertinentes y a la difusión inicial de la información.

El grado de clasificación de la Información Clasificada se determinará de conformidad con lo dispuesto en el ordenamiento jurídico vigente.

La clasificación de seguridad se indicará de forma clara y precisa, independientemente de que la Información Clasificada tratada por el <<ORGANISMO>> sea verbal o figure en soporte de papel, electrónico o cualquier otro.

Las partes constitutivas de un determinado documento (páginas, apartados, secciones, anexos, apéndices o documentos adjuntos) podrán requerir clasificaciones diferentes, lo que deberá indicarse, incluso cuando se almacenen en forma electrónica.

El grado global de clasificación de un documento o archivo deberá ser, al menos, tan alto como el de su componente con mayor grado de clasificación. Cuando se recopile información procedente de diversas fuentes, se revisará el producto final para determinar su grado global de clasificación de seguridad, dado que podría estar justificado un grado de clasificación mayor que el de los componentes que lo forman.

En la medida de lo posible, los documentos que contengan partes con distintos grados de clasificación se estructurarán de tal modo que las partes con un grado de clasificación diferente puedan ser fácilmente reconocidas y separadas, si fuera necesario.

La clasificación de una carta o nota de transmisión de documentos será equivalente al mayor grado de clasificación de los documentos adjuntos. El órgano/organismo originador deberá indicar claramente en qué grado está clasificada la información una vez separada de sus documentos adjuntos mediante la marca correspondiente, según el siguiente ejemplo:

Documento completo: CONFIDENCIAL Sin anexos: DIFUSIÓN LIMITADA

Marcas

Junto con cualquiera de las marcas de clasificación de seguridad señaladas en el presente Procedimiento, la Información Clasificada tratada por el <<ORGANISMO>> podrá llevar marcas adicionales, tales como:

a) Un identificador para designar al órgano/organismo originador (o Responsable de la Información).
b) Cualquier advertencia, código o acrónimo que especifique el ámbito de actividad a que se refiere el documento, así como indicaciones relativas a su distribución específica, basada en el principio de la necesidad de conocer, o a restricciones de su uso.
c) Marcas sobre posibilidad de cesión.
d) En su caso, la fecha o acontecimiento específico tras los cuales podrá rebajarse el grado de clasificación o, incluso, desclasificarse.

Marcas abreviadas de clasificación

Podrán utilizarse marcas de clasificación, abreviadas y normalizadas, para indicar el grado de clasificación de los diferentes apartados de un texto. Las marcas de clasificación completas no se sustituirán por abreviaturas.

Podrán utilizarse dentro de documentos clasificados de la UE las siguientes abreviaturas normalizadas para indicar el grado de clasificación de secciones o bloques del texto de extensión inferior a una página:

Denominación España	Denominación UE	Abreviatura
SECRETO	TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
RESERVADO	SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENCIAL	CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
DIFUSIÓN LIMITADA	RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Producción de Información Clasificada

Cuando se genere un documento clasificado:

a) Cada página llevará claramente marcado el grado de clasificación.
b) Cada página irá numerada.
c) El documento deberá llevar un número de referencia y un asunto, que no constituirá en sí mismo Información Clasificada, salvo que se marque como tal.
d) El documento estará fechado.
e) Los documentos con clasificación RESERVADO o superior llevarán un número de ejemplar en cada página, cuando hayan de distribuirse en varios ejemplares.

Reducción del grado de clasificación y desclasificación de la Información Clasificada tratada por el <<ORGANISMO>>

En el momento de producir la información, el órgano/organismo originador (o el Responsable de la Información) indicará, cuando sea posible y muy especialmente si se trata de Información Clasificada de grado DIFUSIÓN LIMITADA, si el grado de clasificación de la

información puede ser reducido o desclasificado a partir de una determinada fecha o tras un acontecimiento concreto.

La <<U/OC>> de seguridad competente revisará periódicamente la Información Clasificada tratada por el <<ORGANISMO>> para verificar si el grado de clasificación asignado sigue siendo aplicable. La <<U/OC>> de seguridad competente creará un sistema para revisar, con una frecuencia mínima quinquenal, el grado de clasificación de la Información Clasificada registrada tratada por el <<ORGANISMO>> que haya generado. Dicha revisión no será necesaria cuando el órgano/organismo originador (o el Responsable de la Información) haya indicado desde el principio que el grado de clasificación de la información podrá ser automáticamente reducido o que la información podrá desclasificarse, y la información haya sido marcada consecuentemente.

3. REGISTRO DE LA INFORMACIÓN CLASIFICADA TRATADA POR EL <<ORGANISMO>> A EFECTOS DE SEGURIDAD

Todo servicio administrativo de los organismos de las AA.PP en que se maneje Información Clasificada contará con un Registro competente con el fin de garantizar que la Información Clasificada se maneja de conformidad con las disposiciones del presente Procedimiento. Los registros se constituirán como Zonas de Acceso Restringido, tal y como se definen en el Anexo III.

A efectos del presente Procedimiento, por registro a efectos de seguridad (denominado en lo sucesivo «registro») se entenderá la aplicación de procedimientos que registren el ciclo de vida del material de que se trate, incluida su difusión y destrucción.

Todo material clasificado de grado CONFIDENCIAL y superior se inscribirá en registros especiales a su entrada o salida de un servicio administrativo.

En el caso de un Sistema de Información, los procedimientos de registro podrán llevarse a cabo mediante procesos dentro del propio Sistema de Información.

En virtud de lo dispuesto en la Decisión 2011/292/UE, de 31 de marzo, sobre las normas de seguridad para la protección de la información clasificada de la UE, el Consejo de la UE aprobará una política de seguridad sobre el registro de Información Clasificada Europea.

Registros SECRETO

Se establecerá un registro nacional que actuará como principal organismo receptor y emisor de la Información Clasificada de grado SECRETO. Cuando proceda, podrán designarse registros secundarios para manejar dicha información.

Los registros secundarios no podrán transmitir documentos de grado SECRETO directamente a otros registros secundarios dependientes del mismo registro central SECRETO, ni al exterior, sin la autorización expresa y por escrito de este último.

4. COPIA Y TRADUCCIÓN DE DOCUMENTOS CLASIFICADOS DE LA UE

Los documentos de grado SECRETO solo podrán copiarse o traducirse con el consentimiento previo y por escrito del órgano/organismo originador (o el Responsable de la Información.)

Cuando el órgano/organismo originador de documentos clasificados (o el Responsable de la Información) de grado RESERVADO o inferior no haya impuesto ninguna restricción a su copia o traducción, estos documentos podrán copiarse o traducirse por indicación de su poseedor.

Las medidas de seguridad aplicables a los documentos originales serán aplicables a sus copias y traducciones.

5. TRANSPORTE DE INFORMACIÓN CLASIFICADA

El transporte de Información Clasificada estará sujeto a las medidas de protección que se señalan en los puntos siguientes. Cuando se transmita Información Clasificada por medios electrónicos, las medidas de protección que figuran a continuación se completarán con las debidas contramedidas técnicas que prescriba la <<U/OC>> de seguridad competente, a fin de reducir al mínimo el riesgo de pérdida o comprometimiento.

Las autoridades de seguridad competentes de la Secretaría General del Consejo de la UE y de España emitirán instrucciones para el transporte de Información Clasificada conforme a la Decisión 2011/292/UE, de 31 de marzo, sobre las normas de seguridad para la protección de la información clasificada de la UE.

Dentro de un edificio o grupo independiente de edificios

La Información Clasificada tratada por el <<ORGANISMO>> que se transporte dentro de un mismo edificio o grupo independiente de edificios irá cubierta, para evitar que su contenido sea visible.

Dentro de un edificio o grupo independiente de edificios, la Información Clasificada de grado SECRETO se transportará en sobre sellado en el que se indicará únicamente el nombre del destinatario.

Dentro de la UE

La Información Clasificada que se transporte entre edificios o locales de la UE irá empaquetada de forma que quede protegida frente a una revelación no autorizada.

El transporte de Información Clasificada de grado RESERVADO o inferior dentro de la UE se efectuará por uno de los siguientes medios:

a) Correo diplomático, oficial o militar, según proceda.
b) Transporte en mano, siempre que:

   i) la Información Clasificada no deje de estar en posesión del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el anexo III,
   ii) la Información Clasificada no se abra durante el camino ni se lea en lugares públicos,
   iii) se instruya al portador sobre sus responsabilidades en materia de seguridad,
   iv) se entregue al portador un certificado de correo cuando sea necesario;
c) Servicios postales o servicios de mensajería comercial, siempre que:

   i) hayan sido aprobados por la ANS competente, de conformidad con el ordenamiento jurídico español,

ii) apliquen medidas de protección adecuadas de conformidad con los requisitos mínimos que se establezcan en las directrices de seguridad a que se refiere el artículo 6 de la Decisión 2011/292/UE.

Si el transporte se efectúa de un Estado miembro a otro, las disposiciones de la letra c) se aplicarán únicamente a la Información Clasificada hasta el grado CONFIDENCIAL.

El material clasificado de grado CONFIDENCIAL y de grado RESERVADO (por ejemplo, equipamiento o maquinaria) que no pueda transportarse por los medios indicados en el punto anterior deberá ser transportado por empresas comerciales de transporte con arreglo a lo dispuesto en el anexo VI.

El transporte de Información Clasificada de grado SECRETO entre edificios o locales de la UE se efectuará por correo diplomático, oficial o militar, según proceda.

Desde la UE al territorio de un tercer Estado

La Información Clasificada tratada por el <<ORGANISMO>> que se transporte a un tercer Estado, irá empaquetada de forma que quede protegida de una revelación no autorizada.

El transporte de Información Clasificada de grado CONFIDENCIAL y de grado RESERVADO se efectuará por uno de los siguientes medios:

a) Correo diplomático o militar.
b) Transporte en mano, siempre que:

i) el paquete lleve sello oficial, o por sus características indique que se trata de un envío oficial, no debiendo someterse a controles aduaneros o de seguridad,
ii) el portador lleve un certificado de correo, con mención específica del paquete, que le autorice a transportarlo,
iii) la Información Clasificada no deje de estar en posesión del portador, a menos que se almacene de acuerdo con los requisitos establecidos en el Anexo III,
iv) la Información Clasificada no se abra durante el camino ni se lea en lugares públicos, y
v) se instruya al portador sobre sus responsabilidades en materia de seguridad.

El transporte de Información Clasificada de grado CONFIDENCIAL y de grado RESERVADO cedida a un tercer Estado o a una organización internacional deberá atenerse a las disposiciones pertinentes de un acuerdo de seguridad de la información o de un convenio.

La Información Clasificada de grado DIFUSION LIMITADA podrá ser transportada también por servicios postales o servicios de mensajería comercial.

El transporte de Información Clasificada de grado SECRETO hasta el territorio de un tercer Estado se efectuará por correo militar o diplomático.

6. DESTRUCCIÓN DE INFORMACIÓN CLASIFICADA

Los documentos clasificados que hayan dejado de ser necesarios podrán destruirse, sin perjuicio de la normativa sobre archivos que resulte de aplicación.

Los documentos sujetos a registro serán destruidos por el Registro competente, por orden de su poseedor o de una autoridad competente. Los libros de registro y cualquier información relacionada con el registro se actualizarán en su consecuencia.

Cuando se trate de documentos clasificados de grado RESERVADO o SECRETO, la destrucción se realizará en presencia de un testigo, que deberá estar habilitado, al menos, para el grado de clasificación del documento que se vaya a destruir.

El encargado del Registro y el testigo, en caso de que se requiera su presencia, firmarán un certificado de destrucción, que se archivará en el Registro. El Registro conservará los certificados de destrucción de los documentos de grado SECRETO durante, AL MENOS, diez años, y de los documentos de grado CONFIDENCIAL y RESERVADO durante, al menos, cinco años.

Los documentos clasificados, incluidos los de grado DIFUSIÓN LIMITADA, se destruirán por métodos que cumplan las normas pertinentes de la UE o normas equivalentes españolas, a fin de impedir su reconstrucción total o parcial.

La destrucción de los soportes de almacenamiento informático utilizados para la Información Clasificada tratada por el <<ORGANISMO>> se realizará de conformidad con lo dispuesto en el Anexo V.

7. INSPECCIONES Y VISITAS DE EVALUACIÓN

El término “inspección” se empleará para designar toda inspección o visita de evaluación realizada de conformidad con lo señalado en el presente Procedimiento, a fin de verificar la eficacia de las medidas establecidas para la protección de la Información Clasificada tratada por el <<ORGANISMO>>.

Las inspecciones se realizarán, básicamente, para:

a) Asegurarse de que se apliquen las normas mínimas para la protección de la Información Clasificada tratada por el <<ORGANISMO>> establecidas en el presente Procedimiento.
b) Destacar la importancia de la seguridad y de una efectiva gestión del riesgo en las entidades inspeccionadas.
c) Recomendar contramedidas que permitan paliar los efectos específicos de la pérdida de confidencialidad, integridad o disponibilidad de la Información Clasificada, y
d) Reforzar los programas de formación y de sensibilización en materia de seguridad que venga desarrollando la <<U/OC>> de seguridad competente del <<ORGANISMO>>.

Según dispone la Decisión 2011/292/UE, de 31 de marzo, sobre las normas de seguridad para la protección de Información Clasificada de la UE, antes del término de cada año natural, el Consejo de la UE adoptará el programa de inspecciones para el año siguiente. Para el caso español, las fechas concretas de cada inspección se determinarán de común acuerdo con la ANS.

Realización de las inspecciones

Las inspecciones se llevarán a cabo con el fin de comprobar el cumplimiento de las normas, reglamentaciones y procedimientos pertinentes del <<ORGANISMO>> inspeccionado y verificar si las prácticas de dicho organismo se ajustan a los principios básicos y las normas

mínimas establecidas en el presente Procedimiento, y a las disposiciones que rigen el intercambio de Información Clasificada con dicho organismo.

Las inspecciones de seguridad se efectuarán en dos fases:

- **Antes de la inspección** propiamente dicha se celebrará una reunión preparatoria con el <<ORGANISMO>> afectado, si procede.
- Tras esta reunión preparatoria, el equipo de inspección establecerá, de común acuerdo con el organismo afectado, un **programa detallado de inspección** que abarque todos los aspectos de la seguridad. El equipo inspector tendrá acceso a todos los locales, en particular a los registros y puntos de acceso a los Sistemas de Información en los que se maneje Información Clasificada tratada por el <<ORGANISMO>>.

Las inspecciones realizadas en los organismos de las AP.PP. españolas se realizarán bajo la dirección de un equipo conjunto de inspección de la Secretaría General del Consejo de la UE y de la Comisión, en plena colaboración con los funcionarios de la entidad inspeccionada.

Las inspecciones realizadas en terceros Estados u organizaciones internacionales se efectuarán bajo la dirección de un equipo conjunto de inspección de la Secretaría General del Consejo de la UE y de la Comisión, en plena colaboración con los funcionarios del tercer Estado o de la organización internacional inspeccionados.

Las inspecciones de las agencias y órganos de la UE creados en virtud del título V, capítulo 2, del Tratado de la Unión Europea, así como de Europol y Eurojust, serán efectuadas por la Oficina de Seguridad de la Secretaría General del Consejo de la UE, con asistencia de expertos de la ANS del país en que esté establecida la agencia u órgano UE. La Dirección de Seguridad de la Comisión Europea (DSCE) podrá asociarse a la inspección cuando intercambie periódicamente Información Clasificada con la agencia u órgano en cuestión.

En el caso de las inspecciones de agencias y órganos de la UE creados en virtud del título V, capítulo 2, del Tratado de la Unión Europea, así como de Europol y Eurojust, y de terceros Estados y organizaciones internacionales, se solicitará la asistencia y contribución de expertos de la ANS, de conformidad con las medidas de aplicación que debe acordar el Comité Seguridad.

Informes de inspección

Al término de la inspección se presentarán a la entidad inspeccionada las principales conclusiones y recomendaciones. A continuación, se elaborará un Informe de Inspección bajo la responsabilidad de la Oficina de Seguridad de la Secretaría General del Consejo de la UE (en su calidad de organismo de seguridad). Cuando se hayan propuesto medidas correctoras y recomendaciones, el informe incluirá datos suficientes que avalen sus conclusiones. El Informe de Inspección se remitirá a la <<U/OC>> de seguridad competente del <<ORGANISMO>> inspeccionado.

Con respecto a las inspecciones realizadas en las administraciones públicas de los Estados miembros:

a) El proyecto de informe de inspección se remitirá a la ANS para que verifique que no contiene errores en cuanto a los hechos ni Información Clasificada de grado superior a DIFUSIÓN LIMITADA.

b) Salvo cuando la ANS solicite que no se efectúe una difusión general, los informes de inspección se distribuirán a los miembros del Comité de Seguridad y a la DSCE. El informe llevará la clasificación de DIFUSIÓN LIMITADA.

Se elaborará un informe periódico, bajo la responsabilidad de la Oficina de Seguridad de la Secretaría General del Consejo de la UE, para destacar las principales enseñanzas extraídas de las inspecciones realizadas en los Estados miembros a lo largo de un período determinado; el informe será examinado por el Comité de Seguridad.

Cuando se trate de visitas de evaluación de terceros Estados u organizaciones internacionales, el informe se remitirá al Comité de Seguridad y a la DSCE. Esos informes llevarán la clasificación, como mínimo, de DIFUSIÓN LIMITADA. En las visitas de seguimiento se comprobará la aplicación de las medidas correctoras y se informará de ella al Comité de Seguridad.

Cuando se trate de inspecciones de agencias u órganos de la UE creados en virtud del título V, capítulo 2, del Tratado de la Unión Europea, así como de Europol y Eurojust, los informes de inspección se distribuirán a los miembros del Comité de Seguridad y de la DSCE. Los proyectos de informes de inspección se remitirán a la agencia u órgano de que se trate para que verifique que no contienen errores en cuanto a los hechos ni Información Clasificada de grado superior a DIFUSIÓN LIMITADA. En las visitas de seguimiento se comprobará la aplicación de las medidas correctoras y se informará de ella al Comité de Seguridad.

La Oficina de Seguridad de la Secretaría General del Consejo de la UE realizará inspecciones periódicas de los servicios administrativos de la Secretaría General del Consejo de la UE a los fines establecidos anteriormente.

Lista de control para las inspecciones

Corresponderá a la Oficina de Seguridad de la Secretaría General del Consejo de la UE elaborar y actualizar una lista de control para la inspección de seguridad de los puntos que deberán comprobarse en el curso de una inspección. Esta lista y sus eventuales actualizaciones se remitirán al Comité de Seguridad.

La información para completar la lista de control se obtendrá, en particular durante la inspección, de los encargados de la gestión de seguridad de la entidad inspeccionada. Una vez completada con las respuestas detalladas, la lista de control se clasificará de común acuerdo con la entidad inspeccionada. No formará parte del informe de inspección.

ANEXO V

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

1. INTRODUCCIÓN

El presente Anexo establece disposiciones para la protección de la Información Clasificada tratada en los Sistemas de Información del <<ORGANSMO>>.

En el contexto de este Anexo se utilizarán los siguientes conceptos:

Autenticidad: la garantía de que la información es verídica y procede de fuentes de buena fe.
Disponibilidad: la propiedad de ser accesible y utilizable en el momento que lo requiera una entidad autorizada.
Confidencialidad: la propiedad de la información de no ser revelada a personas, organismos o procesos no autorizados;
Integridad: la propiedad de salvaguardar la exactitud y completitud de la información y los activos;
No repudio: la capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente.

2. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Las disposiciones que se establecen a continuación constituyen el punto de partida para garantizar la seguridad del sistema del <<ORGANISMO>> que maneje Información Clasificada. Los requisitos detallados para dar cumplimiento a las presentes disposiciones se definirán en políticas y directrices de seguridad.

Gestión del riesgo de seguridad

La gestión del riesgo de seguridad será parte integrante de la definición, desarrollo, funcionamiento y mantenimiento de los Sistemas de Información del <<ORGANISMO>>. La gestión del riesgo (evaluación, tratamiento, aceptación y comunicación) se llevará a cabo como un proceso iterativo y de forma conjunta por parte de los propietarios del sistema, las autoridades del proyecto, las autoridades operativas y las autoridades responsables de la aprobación de la seguridad, recurriendo a un método de evaluación del riesgo que haya demostrado su eficacia y sea transparente y plenamente comprensible. El alcance del Sistema de Información y de sus activos estará claramente definido ya desde el comienzo del proceso de gestión del riesgo.

La <<U/OC>> de seguridad competente del <<ORGANISM>> examinará las amenazas potenciales para el Sistema de Información y mantendrá actualizadas las evaluaciones de la amenazas, de modo que reflejen el entorno operativo del momento. Actualizará continuamente sus conocimientos de las cuestiones relativas a la vulnerabilidad y revisará periódicamente la evaluación de la vulnerabilidad para hacer frente al entorno cambiante de las tecnologías de la información.

El tratamiento del riesgo de seguridad tendrá por objeto aplicar un conjunto de medidas de seguridad que creen un equilibrio satisfactorio entre las necesidades de los usuarios, el coste y el riesgo residual.

Los requisitos específicos, escala y grado de detalle determinados por la autoridad de acreditación de seguridad pertinente para acreditar el Sistema de Información serán proporcionales al riesgo evaluado, teniendo en cuenta todos los factores pertinentes, con inclusión del grado de clasificación de la Información Clasificada tratada por el <<ORGANISMO>>. La acreditación incluirá una declaración formal sobre el riesgo residual y la aceptación de dicho riesgo por parte de una autoridad competente.

Seguridad a lo largo del ciclo de vida del SIC

Garantizar la seguridad constituirá un requisito a lo largo de todo el ciclo de vida del Sistema de Información, desde su comienzo hasta su retirada del servicio.

Para cada fase del ciclo de vida de un sistema, se determinará el papel y la interacción de todo participante en el Sistema de Información con respecto a su seguridad.

Cualquier Sistema de Información del <<ORGANISMO>>, incluidas sus medidas de seguridad de carácter técnico y no técnico, será objeto de pruebas de seguridad durante su proceso de acreditación, para asegurarse de que se obtiene el nivel adecuado de garantía y verificar que esos sistemas están correctamente aplicados, integrados y configurados.

Se realizarán periódicamente evaluaciones, inspecciones y exámenes de seguridad durante el funcionamiento y el mantenimiento del Sistema de Información y cuando se produzcan circunstancias excepcionales.

La documentación de seguridad de un Sistema de Información irá evolucionando a lo largo de su ciclo de vida como parte integrante del proceso de gestión de la configuración y del cambio.

Mejores prácticas

La Secretaría General del Consejo de la UE y los Estados miembro (a través de la ANS) colaborarán en el desarrollo de mejores prácticas para la protección de la Información Clasificada tratada por los organismos públicos de la UE. Las directrices sobre las mejores prácticas establecerán medidas de seguridad técnicas, físicas, de organización y de procedimiento para los Sistemas de Información, de probada eficacia para contrarrestar determinadas amenazas y vulnerabilidades.

La protección de la Información Clasificada tratada por el <<ORGANISMO>> se basará en las enseñanzas obtenidas por las entidades que intervienen en la Seguridad de la Información tanto dentro de la UE como fuera de ella.

La difusión y ulterior aplicación de las mejores prácticas contribuirán a lograr un nivel equivalente de garantía en los distintos Sistemas de Información que manejan Información Clasificada y que funcionan en la Secretaría General del Consejo de la UE y en los Estados miembros.

Defensa en profundidad

Para paliar los riesgos en los Sistemas de Información, se aplicarán una serie de medidas de seguridad de carácter técnico y no técnico, organizadas a modo de defensa en barreras sucesivas. Esas barreras incluirán:

a) *Disuasión:* medidas de seguridad destinadas a desalentar a los adversarios que planeen un ataque a un Sistema de Información.

b) *Prevención:* medidas de seguridad destinadas a impedir u obstaculizar un ataque a un Sistema de Información.
c) *Detección:* medidas de seguridad destinadas a descubrir que se ha producido un ataque a un Sistema de Información.
d) *Resiliencia:* medidas de seguridad destinadas a limitar las consecuencias de un ataque a un conjunto mínimo de información o de activos de un Sistema de Información y a impedir mayores daños, y
e) *Recuperación:* medidas de seguridad destinadas a volver al estado anterior de seguridad del Sistema de Información.

El grado de rigor de estas medidas de seguridad se determinará mediante una evaluación del riesgo.

La <<U/OC>> de seguridad competente se asegurará de poder responder a incidentes que puedan traspasar los límites de las organizaciones o las fronteras nacionales, con el fin de coordinar las respuestas y compartir información sobre dichos incidentes y los riesgos conexos (capacidades de respuesta para urgencias informáticas).

Principio de privilegios mínimos

Únicamente se pondrán en marcha las funciones, dispositivos y servicios esenciales para cubrir las necesidades operativas del <<ORGANISMO>>, con el fin de evitar riesgos innecesarios.

Los usuarios de los Sistemas de Información y los procesos automáticos solo obtendrán el acceso, los privilegios o los permisos que necesiten para realizar su cometido, con el fin de limitar los daños resultantes de accidentes, errores o uso no autorizado de recursos de los Sistemas de Información.

Los procedimientos de registro que efectúe un Sistema de Información, cuando es preciso, se verificarán como parte del proceso de acreditación.

Concienciación de la Seguridad de la Información

La conciencia de los riesgos y de las medidas de seguridad disponibles constituye la primera línea de defensa de la seguridad de los Sistemas de Información. En particular, todas las personas que intervienen en el ciclo de vida de uno de tales sistemas, incluidos sus usuarios, deben ser conscientes:

a) De que los fallos de seguridad pueden perjudicar seriamente al propio Sistema de Información.
b) De los posibles daños a terceros que pueden derivarse de la interconecxión e interdependencia, y
c) De que son responsables de la seguridad del Sistema de Información y se les exigirá la responsabilidad debida según la función que desempeñen en los sistemas y procesos.

Para garantizar que son conscientes de las responsabilidades que conlleva la seguridad, será obligatoria la formación y concienciación en relación con la Seguridad de la Información para todo el personal implicado, tanto los altos directivos como los usuarios de los Sistemas de Información.

Evaluación y aprobación de los productos de seguridad

El grado de confianza necesario en las medidas de seguridad, definido como nivel de garantía, se determinará con arreglo al resultado del proceso de gestión del riesgo y en consonancia con las correspondientes políticas y directrices de seguridad.

El nivel de garantía se verificará recurriendo a procedimientos y metodologías reconocidos internacionalmente o aprobados en el plano nacional. Aquí deben incluirse principalmente la evaluación, los controles y las auditorías.

Los productos criptológicos de protección de la Información Clasificada tratada por el <<ORGANISMO>> serán evaluados y aprobados por la ANS.

Antes de recomendarlos para su aprobación por el Consejo o el Secretario General, de conformidad con el artículo 10, apartado 6 de la Decisión 2011/292/UE, dichos productos criptológicos deberán superar una segunda evaluación realizada por la autoridad debidamente acreditada (ADA) de un Estado miembro que no haya participado en el diseño o fabricación del equipo considerado. El grado de detalle exigido en la segunda evaluación dependerá del grado máximo de clasificación de la Información Clasificada que se prevé proteger con dichos productos. El Consejo de Europa aprobará una política de seguridad sobre la evaluación y aprobación de los productos criptológicos.

Cuando ello esté justificado por motivos operativos específicos, el Consejo de Europa o su Secretario General, según proceda, podrá, previa recomendación del Comité de Seguridad, dispensar del cumplimiento de los requisitos recogidos en los puntos anteriores y otorgar una aprobación provisional durante un período específico, de conformidad con el procedimiento establecido en el artículo 10, apartado 6 de la Decisión 2011/292/UE.

Un ADA será una ACC de un Estado miembro, acreditada mediante criterios objetivos establecidos por el Consejo de Europa para realizar la segunda evaluación de los productos criptológicos de protección de la Información Clasificada.

El Consejo de Europa aprobará una política de seguridad sobre la cualificación y aprobación de productos de seguridad IT no criptológicos.

Transmisión dentro de Zonas de Acceso Restringido

No obstante las disposiciones del presente Procedimiento, cuando la transmisión de Información Clasificada tratada por el <<ORGANISMO>> se limite a Zonas de Acceso Restringido, podrá utilizarse la difusión no cifrada, o cifrada en un nivel inferior, en base al resultado de un proceso de gestión del riesgo y previa aprobación de la AAS.

Interconexión segura de los SIC

A los efectos del presente Procedimiento, por "interconexión" se entenderá la conexión directa de dos o más sistemas IT con objeto de compartir datos y otros recursos de información, de forma unidireccional o multidireccional.

Todo Sistema de Información tratará como no fiable a cualquier sistema IT interconectado y aplicará medidas protectoras para controlar el intercambio de Información Clasificada.

Con relación a todas las interconexiones de un Sistema de Información con otro sistema IT, se observarán los siguientes requisitos básicos:

a) Las autoridades competentes enunciarán y aprobarán los requisitos operacionales o de servicio de dichas interconexiones.

b) La interconexión se someterá a un proceso de gestión del riesgo y acreditación y necesitará la aprobación de las autoridades de acreditación de seguridad competentes, y
c) Se pondrán en marcha servicios de protección del perímetro de todos los Sistemas de Información.

No habrá interconexión entre un Sistema de Información acreditado y una red desprotegida o pública, salvo cuando el Sistema de Información tenga instalado a tal fin un servicio de protección de perímetro aprobado, que actúe entre el sistema y la red desprotegida o pública. Las medidas de seguridad de tales interconexiones serán examinadas por la autoridad de Seguridad de la Información competente y aprobadas por la autoridad de acreditación de seguridad competente.

Cuando la red desprotegida o pública se utilice únicamente para el transporte y los datos estén cifrados con un producto criptológico aprobado en conformidad con el artículo 10 de la Decisión 2011/292/UE, se considerará que la conexión no es una interconexión.

Quedarán prohibidas las interconexiones directas o dispuestas en cascada de un Sistema de Información acreditado para manejar Información Clasificada de grado SECRETO con redes públicas o desprotegidas.

Soportes de almacenamiento informático

Los soportes de almacenamiento informático se destruirán con arreglo a un procedimiento aprobado por la <<U/OC>> de seguridad competente.

La reutilización, la reducción del grado de clasificación y la desclasificación de los soportes de almacenamiento informático se efectuarán de conformidad con una política de seguridad establecida de conformidad con el artículo 6, apartado 1 de la Decisión 2011/2927UE.

Circunstancias de emergencia

No obstante lo dispuesto en el presente Procedimiento, podrán aplicarse los procedimientos específicos que se describen a continuación en casos de emergencia, por ejemplo, en situaciones de crisis, conflicto o guerra, inminentes o reales, o en circunstancias operativas excepcionales.

La Información Clasificada tratada por el <<ORGANISMO>> podrá transmitirse utilizando productos criptológicos que hayan sido certificados para un grado de clasificación inferior o sin cifrar con el consentimiento de la autoridad competente, si resulta evidente que un retraso podría causar un daño superior al que acarrea la revelación del material clasificado y si:

a) El emisor y el receptor carecen de los medios de cifra requeridos o carecen de todo medio de cifra, y
b) El material clasificado no puede transmitirse a tiempo por otros medios.

En las circunstancias expuestas, la Información Clasificada transmitida no llevará ninguna marca ni indicación que la distinga de la información no clasificada o que pueda protegerse mediante un producto criptológico disponible. Se notificará sin demora a los receptores el grado de clasificación, recurriendo a otros medios.

Si hubiera que recurrir a lo expuesto con anterioridad, se presentará posteriormente un informe a la ANS.

3. SEGURIDAD DE LA INFORMACIÓN: FUNCIONES Y AUTORIDADES

En los Estados miembros y en la Secretaría General del Consejo de la UE se establecerán las siguientes funciones respecto de la Seguridad de la Información. Estas funciones no necesitan ser desempeñadas por organismos específicos y únicos. Tendrán cometidos separados. Sin embargo, dichas funciones y sus responsabilidades conexas podrán combinarse o integrarse en el mismo servicio administrativo, o dividirse entre varios de ellos, siempre que se eviten los conflictos internos de intereses o de funciones.

Autoridad de Seguridad de la Información[15]

Corresponderá a la autoridad de Seguridad de la Información:

a) Establecer políticas y directrices de seguridad relativas a la Seguridad de a Información y supervisar su eficacia y pertinencia.
b) Salvaguardar y administrar la información técnica relacionada con los productos criptológicos.
c) Garantizar que las medidas de Seguridad de la Información seleccionadas para proteger la Información Clasificada cumplan las normas que rigen su idoneidad y selección.
d) Garantizar que los productos criptológicos se seleccionen de conformidad con las normas que rigen su idoneidad y selección.
e) Coordinar la formación y la concienciación respecto de la Seguridad de la Información.
f) Consultar al proveedor del sistema, a los actores en el ámbito de la seguridad y a los representantes de los usuarios sobre las políticas y directrices de seguridad relativas a la Seguridad de la Información, y
g) Velar por que se disponga de los conocimientos necesarios en la subsección especializada del Comité de Seguridad para cuestiones de Seguridad de la Información.

Autoridad TEMPEST

Corresponderá a la autoridad TEMPEST garantizar que los Sistemas de Información cumplan las políticas y directrices TEMPEST. La autoridad TEMPEST aprobará contramedidas para instalaciones y productos destinados a proteger Información Clasificada de un determinado grado de clasificación dentro de su entorno operativo.

[15] Competencias que en España corresponden a la Autoridad Nacional de Seguridad – Oficina de Seguridad Nacional, del Centro Nacional de Inteligencia.

Autoridad de certificación criptológica[16]

Corresponderá a la ACC garantizar que los productos criptológicos cumplan la política criptológica nacional o la del Consejo de Europa. Dará su aprobación a los productos criptológicos para tratar Información Clasificada de un determinado grado de clasificación dentro de su entorno operativo. Por lo que se refiere a los Estados miembros, la autoridad de certificación criptológica se encargará de evaluar los productos criptológicos.

Autoridad de distribución criptológica

Corresponderá a la autoridad de distribución criptológica:

a) Gestionar y contabilizar el material criptológico de la UE.
b) Garantizar que se establezcan y apliquen los procedimientos y cauces adecuados para la contabilidad, manejo, almacenamiento y distribución de todo el material criptológico de la UE, y
c) Garantizar la transferencia del material criptológico de la UE entre las personas o servicios que lo empleen.

Autoridad de acreditación de seguridad

Corresponderá a la autoridad de acreditación de seguridad de cada sistema:

a) Velar por que los Sistemas de Información cumplan las políticas y directrices de seguridad pertinentes, expedir una declaración de aprobación a los Sistemas de Información para manejar Información Clasificada tratada de un determinado grado de clasificación en su entorno operativo, en la que se declaren las condiciones de la acreditación y los criterios aplicables para exigir una nueva aprobación.
b) Establecer un proceso de acreditación de seguridad, de conformidad con las políticas pertinentes, que enuncie claramente las condiciones de aprobación de los Sistemas de Información bajo su autoridad.
c) Definir una estrategia de acreditación de seguridad que indique el grado de detalle para el proceso de acreditación según el nivel de garantía requerido.
d) Examinar y aprobar la documentación de seguridad, incluidas las declaraciones de gestión del riesgo y de riesgo residual, las declaraciones de requisitos específicos de seguridad del sistema, la documentación relativa a la verificación de la aplicación de

[16] Entre las funciones que el Real Decreto 421/2004, de 12 de marzo, asigna al Centro Criptológico Nacional (CCN), está la de "constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, de aplicación a productos y sistemas en su ámbito". Este Organismo de Certificación (OC), en lo relativo a la certificación funcional de la seguridad de las TI, se articuló mediante el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por Orden PRE/2740/2007, de 19 de septiembre, completado por su propia normativa interna adaptada a los requisitos necesarios para ser reconocido tanto a nivel nacional, según la norma EN45011, como a nivel internacional, de acuerdo con el «Arreglo de Reconocimiento de Certificados de Criterios Comunes» (CCRA), como entidad de certificación de la seguridad de las TIC.
Para la certificación criptológica y para la certificación TEMPEST, el Organismo de Certificación se basa en criterios y metodologías propias.

la seguridad y los procedimientos operativos de seguridad y asegurarse de que se cumplan las normas y políticas de seguridad del Consejo de Europa.

e) Comprobar la aplicación de las medidas de seguridad en relación con los Sistemas de Información realizando o patrocinando evaluaciones de seguridad, inspecciones o exámenes.
f) Aprobar los criterios de seguridad (por ejemplo, los grados de habilitación del personal) para puestos sensibles en relación con los Sistemas de Información.
g) Refrendar la selección de productos criptológicos y TEMPEST aprobados para dotar de seguridad a los Sistemas de Información.
h) Aprobar la interconexión entre varios Sistemas de Información o, cuando proceda, participar en la aprobación conjunta de dicha interconexión, y
i) Consultar al proveedor del sistema, a los actores en el ámbito de la seguridad y a los representantes de los usuarios respecto de la gestión del riesgo, en particular el riesgo residual, así como sobre las condiciones de la declaración de aprobación.

Corresponderá a la AAS de la Secretaría General del Consejo de la UE la acreditación de todos los SIC que funcionen en el marco del mandato de la Secretaría General del Consejo de la UE.

Corresponderá a la AAS competente de un Estado miembro acreditar los Sistemas de Información y los componentes de estos que operen dentro de su jurisdicción.

Un Panel de Acreditación de Seguridad se encargará de la acreditación de los Sistemas de Información que entren dentro de la competencia tanto de la AAS de la Secretaría General del Consejo de la UE como de las AAS de los Estados miembros. Estará integrado por un representante de la AAS de cada Estado miembro, y asistirá a él un representante de la AAS de la Comisión. Se invitará a asistir a otras entidades conectadas a un SIC, cuando dicho sistema se someta a debate.

El Panel de Acreditación de Seguridad estará presidido por un representante de la AAS de la Secretaría General del Consejo de la UE. Se pronunciará por consenso de los representantes de las AAS de las instituciones, de los Estados miembros y de otras entidades conectados al Sistema de Información de que se trate. Elaborará informes periódicos sobre sus actividades, destinados al Comité de Seguridad y le comunicará todas las declaraciones de acreditación.

Autoridad operacional de Seguridad de la Información

Corresponderá a la autoridad operacional de Seguridad de la Información de cada sistema:

a) Elaborar documentación de seguridad en consonancia con las políticas y directrices de seguridad, en particular con los requisitos específicos de seguridad del sistema, incluida la declaración sobre el riesgo residual, los procedimientos operativos de seguridad y el plan criptológico en el proceso de acreditación de Sistemas de Información.
b) Participar en la selección y ensayo de las medidas técnicas de seguridad específicas para el sistema, de los dispositivos y los programas informáticos; supervisar su aplicación y garantizar que su instalación, configuración y mantenimiento sean seguros, de conformidad con la correspondiente documentación de seguridad.
c) Participar en la selección de medidas de seguridad y dispositivos TEMPEST si lo requiere la enunciación de requisitos específicos de seguridad del sistema y garantizar

que su instalación y mantenimiento sean seguros, en colaboración con la autoridad TEMPEST.

d) Supervisar el cumplimiento y aplicación de los procedimientos operativos de seguridad y, cuando proceda, delegar las competencias sobre la seguridad operativa en el propietario del sistema.
e) Gestionar y manejar productos criptológicos, garantizando la custodia de los artículos criptológicos y controlados y, si es preciso, garantizar la generación de variables criptológicas.
f) Realizar análisis, exámenes y ensayos en materia de seguridad, en particular para elaborar los correspondientes informes sobre el riesgo, cuando lo requiera la autoridad de acreditación de seguridad.
g) Proporcionar formación sobre la Seguridad de la Información específica para los Sistemas de Información.
h) Aplicar y ejecutar medidas de seguridad específicas para los Sistemas de Información.

ANEXO VI

SEGURIDAD INDUSTRIAL

1. INTRODUCCIÓN

El presente Anexo establece disposiciones generales en materia de seguridad aplicables a las sociedades industriales y otro tipo de entidades, en las negociaciones precontractuales y durante la duración de los Contratos Clasificados adjudicados por la Secretaría General del Consejo de la UE.

El Consejo de Europa aprobará una política sobre seguridad industrial que defina, en particular, requisitos detallados en relación con las habilitaciones de seguridad de establecimiento, las cláusulas sobre aspectos de la seguridad, las visitas y la transmisión y el transporte de Información Clasificada.

2. ELEMENTOS DE SEGURIDAD EN UN CONTRATO CLASIFICADO

Guía de clasificación de seguridad

Antes de convocar una licitación o adjudicar un Contrato Clasificado, la Secretaría General del Consejo de la UE, como autoridad contratante, determinará la clasificación de seguridad de toda información que deba proporcionarse a los licitadores y contratistas, así como la clasificación de seguridad de toda información que haya de producir el contratista. Para ello, la Secretaría General del Consejo de la UE elaborará una guía de clasificación de seguridad, que deberá emplearse en la ejecución del contrato.

Para determinar la clasificación de seguridad de los diversos elementos de un contrato clasificado se aplicarán los principios siguientes:

a) Al elaborar una guía de clasificación de seguridad, la Secretaría General del Consejo de la UE tendrá en cuenta todos los aspectos de seguridad pertinentes, incluida la clasificación de seguridad atribuida a la información que se facilite y apruebe para ser utilizada en el contrato en cuestión por el originador de la información.
b) El grado general de clasificación del contrato no podrá ser inferior al mayor grado de clasificación de cualquiera de sus elementos, y
c) Cuando proceda, en caso de que se produzca algún cambio en relación con la clasificación de la información producida por los contratistas o que se les haya facilitado en la ejecución de un contrato, y cuando se introduzca cualquier cambio ulterior en la guía de clasificación de seguridad, la Secretaría General del Consejo de la UE actuará de enlace con la ANS española o cualquier otra autoridad nacional de seguridad afectada.

Cláusula sobre aspectos de la seguridad

Los requisitos de seguridad específicos de un contrato se describirán en una cláusula sobre aspectos de la seguridad, la cual, cuando proceda, incluirá una guía de clasificación de seguridad y será parte integrante del contrato o subcontrato clasificado.

La cláusula sobre aspectos de la seguridad incluirá asimismo las disposiciones que exigirán del contratista o subcontratista el cumplimiento de los estándares mínimos que se establecen en la Decisión 2011/292/UE. El incumplimiento de dichos estándares mínimos podrá ser motivo suficiente para la rescisión del contrato.

Instrucciones de seguridad de un programa o proyecto

Según cuál sea el ámbito de los programas o proyectos que conlleven acceso a Información Clasificada o su manejo o almacenamiento, la autoridad contratante designada para gestionar el programa o proyecto podrá emitir unas instrucciones de seguridad específicas del programa o proyecto. Estas instrucciones requerirán la aprobación de la ANS española o de cualquier otra autoridad de seguridad competente que participen en un determinado proyecto o programa, y podrán contener requisitos de seguridad adicionales.

3. HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO

La habilitación de seguridad de establecimiento será concedida por la ANS española para indicar, de conformidad con el ordenamiento jurídico español, que una sociedad industrial u otro tipo de entidad puede proteger dentro de sus instalaciones la Información Clasificada del grado de clasificación que corresponda (CONFIDENCIAL o RESERVADO). Dicha habilitación se presentará a la Secretaría General del Consejo de la UE, como autoridad contratante, antes de facilitar o conceder acceso a la Información Clasificada a un contratista o subcontratista, o a un posible contratista o subcontratista.

Al expedir una habilitación de seguridad de establecimiento, la ANS española procederá, como mínimo, a:

a) Evaluar la integridad de la sociedad industrial u otro tipo de entidad.
b) Evaluar la propiedad, el control o cualquier posible influencia indebida que pueda considerarse un riesgo para la seguridad.
c) Verificar que la sociedad industrial u otro tipo de entidad ha implantado un sistema de seguridad en el establecimiento que aplica todas las medidas de seguridad apropiadas necesarias para la protección de la información o el material clasificados de grado CONFIDENCIAL o RESERVADO, de conformidad con los requisitos prescritos en la decisión 2011/292/UE.
d) Verificar que la situación de seguridad de los directivos, los propietarios y los empleados que necesitan acceder a Información Clasificada de grado CONFIDENCIAL o RESERVADO se ha establecido de conformidad con los requisitos prescritos en la Decisión 2011/292/UE.
e) Verificar que la sociedad industrial u otro tipo de entidad ha nombrado un agente de seguridad del establecimiento, que responda ante su dirección de la observancia de las obligaciones en cuanto a la seguridad.

Cuando proceda, la Secretaría General del Consejo de la UE, como autoridad contratante, comunicará a la ANS española que es necesario contar con una habilitación de seguridad de establecimiento en la fase precontractual o para la ejecución del contrato. En la fase precontractual, será necesaria una habilitación de seguridad de establecimiento o una HPS cuando durante el proceso de licitación deba facilitarse Información Clasificada de los grados CONFIDENCIAL o RESERVADO.

La autoridad contratante no adjudicará un Contrato Clasificado al licitador seleccionado antes de haber recibido de la ANS del Estado miembro en que esté registrado el contratista o

subcontratista confirmación de que se ha expedido a este la habilitación de seguridad de establecimiento adecuada.

La ANS española, cuando haya expedido una habilitación de seguridad de establecimiento, notificará a la Secretaría General del Consejo de la UE, como autoridad contratante, los cambios que afecten a dicha habilitación. En el caso de los subcontratos, se informará al respecto a la ANS española.

La retirada de una habilitación de seguridad de establecimiento por parte de la ANS constituirá motivo suficiente para que la Secretaría General del Consejo de la UE, como autoridad contratante, rescinda un contrato clasificado o excluya a un licitador de la licitación.

4. CONTRATOS Y SUBCONTRATOS CLASIFICADOS

Cuando se facilite Información Clasificada a un licitador en la fase precontractual, el pliego de condiciones deberá contener una cláusula que obligue a los licitadores que no presenten ofertas o que no resulten seleccionados a devolver toda la documentación clasificada en un plazo determinado.

Una vez que se haya adjudicado un contrato o subcontrato clasificado, la Secretaría General del Consejo de la UE, como autoridad contratante, notificará a la ANS del Estado del contratista o subcontratista, las disposiciones de seguridad del contrato clasificado.

En caso de rescisión de un contrato de este tipo, la Secretaría General del Consejo de la UE, como autoridad contratante (o la ANS, la ASD o cualquier otra autoridad de seguridad competente, según proceda, en el caso de una subcontratación), lo notificarán cuanto antes a los correspondientes organismos o autoridades competentes del Estado miembro en que esté registrado el contratista o subcontratista.

Por regla general, el contratista o subcontratista estará obligado a devolver a la autoridad contratante, al término del contrato o subcontrato clasificado, toda la Información Clasificada que obre en su posesión.

La cláusula sobre aspectos de la seguridad establecerá disposiciones específicas para la eliminación de Información Clasificada durante la ejecución del contrato o al término de este.

Cuando el contratista o subcontratista esté autorizado a conservar Información Clasificada tras la terminación de un contrato, seguirán siendo de aplicación las normas mínimas contenidas en la Decisión 2011/292/UE y el contratista o subcontratista protegerá la confidencialidad de la Información Clasificada.

Las condiciones en que un contratista podrá subcontratar se definirán en el pliego de condiciones y en el contrato.

Antes de subcontratar cualquier parte de un contrato clasificado, el contratista deberá obtener de la Secretaría General del Consejo de la UE, como autoridad contratante, el permiso correspondiente. No podrá adjudicarse un subcontrato a sociedades industriales u otro tipo de entidades registradas en un Estado que no sea miembro de la UE y no haya celebrado un acuerdo de seguridad de la información con esta.

El contratista responderá de que todas las actividades subcontratadas se ejecuten de conformidad con las normas mínimas prescritas en la Decisión 2011/292/UE y no transmitirá Información Clasificada a ningún subcontratista sin el previo consentimiento escrito de la autoridad contratante.

Respecto de la Información Clasificada producida o manejada por el contratista o subcontratista, los derechos que asistan al originador serán ejercidos por la autoridad contratante.

5. VISITAS EN RELACIÓN CON CONTRATOS CLASIFICADOS

Cuando la Secretaría General del Consejo de la UE, los contratistas o los subcontratistas necesiten acceder a Información Clasificada de los grados CONFIDENCIAL o RESERVADO que se halle en los locales de los otros para la ejecución de un Contrato Clasificado, se organizarán visitas, en contacto con la ANS española. No obstante, en el contexto de proyectos específicos, la ANS española podrá también acordar un procedimiento que permita organizar directamente dichas visitas.

Todos los visitantes deberán estar en posesión de una HPS y tener "Necesidad de Conocer" para poder acceder a la Información Clasificada relacionada con el contrato de la Secretaría General del Consejo de la UE.

A los visitantes solo se les permitirá el acceso a Información Clasificada que guarde relación con la finalidad de la visita.

6. TRANSMISIÓN Y TRANSPORTE DE INFORMACIÓN CLASIFICADA

Por lo que se refiere a la transmisión de Información Clasificada por medios electrónicos, se aplicarán las disposiciones pertinentes del artículo 10 de la Decisión 2011/292/U y lo contenido en el presente Procedimiento.

Por lo que se refiere al transporte de Información Clasificada, se aplicarán las disposiciones pertinentes del Anexo V, de conformidad con el ordenamiento jurídico.

Por lo que se refiere al transporte como carga de material clasificado, se aplicarán los siguientes principios para determinar los planes de seguridad:

a) La seguridad deberá estar garantizada durante todas las fases del transporte, desde el punto de origen hasta el destino final.
b) El grado de protección concedido a un envío se determinará en función del mayor grado de clasificación del material que contenga.
c) Se obtendrá una habilitación de seguridad de establecimiento del grado adecuado para las sociedades encargadas del transporte. En esos casos, el personal que se ocupe del envío deberá estar habilitado de conformidad con el Anexo II.
d) Antes de efectuarse cualquier traslado transfronterizo de material clasificado de los grados CONFIDENCIAL o RESERVADO, el remitente elaborará un plan de transporte que deberá ser aprobado por la ANS.
e) En la medida de lo posible, los viajes evitarán las paradas intermedias y se completarán con toda la rapidez que las circunstancias permitan.
f) Siempre que sea posible, se circulará exclusivamente a través de Estados miembros. Solo deberán emplearse itinerarios que atraviesen Estados no miembros de la UE previa autorización de la ANS o cualquier otra autoridad de seguridad competente tanto del Estado remitente como del destinatario.

7. TRANSMISIÓN DE INFORMACIÓN CLASIFICADA A CONTRATISTAS ESTABLECIDOS EN TERCEROS ESTADOS

La transmisión de Información Clasificada a contratistas y subcontratistas establecidos en terceros Estados se hará de conformidad con las medidas de seguridad que adopten de común acuerdo la Secretaría General del Consejo de la UE, como autoridad contratante, y la ANS del tercer Estado afectado en que esté registrado el contratista.

8. MANEJO Y ALMACENAMIENTO DE INFORMACIÓN CLASIFICADA DE GRADO DIFUSIÓN LIMITADA

La Secretaría General del Consejo de la UE, como autoridad contratante, en colaboración con la ANS española, según proceda, estará facultada para realizar visitas a los establecimientos de los contratistas o subcontratistas en virtud de disposiciones contractuales, con el fin de cerciorarse de que se aplican las medidas de seguridad adecuadas para la protección de la Información Clasificada DIFUSIÓN LIMITADA, tal como se haya estipulado en el contrato.

En la medida necesaria, y de conformidad con el ordenamiento jurídico nacional, la Secretaría General del Consejo de la UE, como autoridad contratante, notificará a la ANS o cualquier otra autoridad de seguridad competente los contratos o subcontratos que contengan Información Clasificada de grado DIFUSIÓN LIMITADA.

Para los contratos adjudicados por la Secretaría General del Consejo de la UE que contengan Información Clasificada de grado DIFUSIÓN LIMITADA, no se exigirá a los contratistas o subcontratistas ni a su personal una habilitación de seguridad de establecimiento ni una HPS.

La Secretaría General del Consejo de la UE, como autoridad contratante, estudiará las respuestas a las invitaciones a presentar ofertas para los contratos que requieran el acceso a Información Clasificada de grado DIFUSIÓN LIMITADA, independientemente de los requisitos relativos a una habilitación de seguridad de establecimiento o una HPS que puedan exigir las disposiciones legales y reglamentarias nacionales.

Las condiciones en que el contratista podrá subcontratar deberán estar en conformidad con las expresadas anteriormente.

Cuando un contrato suponga el manejo de Información Clasificada de grado DIFUSIÓN LIMITADA en un Sistema de Información gestionado por un contratista, la Secretaría General del Consejo de la UE, como autoridad contratante, garantizará que en el contrato o en cualquier posible subcontrato se detallen los requisitos técnicos y administrativos necesarios para la acreditación del Sistema de Información que sean acordes al riesgo evaluado, teniendo en cuenta todos los factores pertinentes. El ámbito de la acreditación de dicho Sistema de Información se determinará mediante acuerdo entre la autoridad contratante y la ANS.

ANEXO VII

INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES

1. INTRODUCCIÓN

El presente Anexo establece disposiciones para el intercambio de Información Clasificada con terceros Estados y organizaciones internacionales.

2. MARCOS QUE REGULAN EL INTERCAMBIO DE INFORMACIÓN CLASIFICADA

Cuando el Consejo de Europa 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 12, apartado 2, y las secciones III y IV de la Decisión 2011/292/UE y sobre la base de una recomendación del Comité de Seguridad.

Cuando la Información Clasificada generada a efectos de una operación PCSD [17] 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 Información Clasificada con el tercer Estado u organización internacional de que se trate se regulará, conforme a lo dispuesto en el epígrafe 5, por:

- Un acuerdo marco de participación,
- Un acuerdo de participación *ad hoc*, o
- De no existir alguno de estos, un acuerdo administrativo *ad hoc*.

En ausencia de uno de los marcos a que se refieren los puntos anteriores, y cuando se adopte la decisión de ceder Información Clasificada a un tercer Estado u organización internacional con arreglo a un procedimiento *ad hoc* de carácter excepcional de conformidad con lo dispuesto en el epígrafe 6, se pedirán garantías por escrito al tercer Estado u organización internacional interesado de que mantendrá protegida la Información Clasificada que se le ceda de acuerdo con los principios básicos y las normas mínimas establecidas por la Decisión 2011/292/UE.

3. ACUERDOS DE SEGURIDAD DE LA INFORMACIÓN

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

[17] Una operación militar o civil de gestión de crisis en virtud del título V, capítulo 2, del Tratado de la UE.

Los acuerdos de seguridad de la información establecerán las disposiciones técnicas de aplicación que deban convenirse entre la Oficina de Seguridad de la Secretaría General del Consejo de la UE, la DSCE y la autoridad competente en materia de seguridad del tercer Estado u organización internacional de que se trate. Dichas disposiciones, que deberán ser aprobadas por el Comité de Seguridad, deberán tener 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.

No se intercambiará Información Clasificada por medios electrónicos a menos que se haya previsto explícitamente en el acuerdo de seguridad de la información o en las disposiciones técnicas de aplicación.

Los acuerdos de seguridad de la información establecerán que, antes de intercambiarse la Información Clasificada en virtud del acuerdo, la Oficina de Seguridad de la Secretaría General del Consejo de la UE y la DSCE acordarán que la parte receptora es capaz de proteger y salvaguardar adecuadamente la información que se le haya facilitado.

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

Con el fin de evaluar la eficacia de las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional en cuestión, la Oficina de Seguridad de la Secretaría General del Consejo de la UE, junto con la DSCE y de común acuerdo con el tercer Estado o la organización internacional de que se trate, efectuarán visitas de evaluación. Dichas visitas se realizarán de conformidad con las disposiciones pertinentes del Anexo IV 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 Información Clasificada que ha de cederse.

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

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

Deberá ponerse el máximo empeño en realizar una inspección de seguridad completa 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 Secretaría General del Consejo de la UE, 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.

El Comité de Seguridad podrá decidir que, mientras no se hayan examinado los resultados de una visita de evaluación, no se ceda Información Clasificada, o solo hasta un nivel determinado, o podrá fijar otras condiciones específicas para la cesión de Información Clasificada al tercer Estado o a la organización internacional. Ello será notificado por la Oficina de Seguridad de la Secretaría General del Consejo de la UE al tercer Estado o a la organización internacional de que se trate.

De mutuo acuerdo con el tercer Estado o la organización internacional, la Oficina de Seguridad de la Secretaría General del Consejo de la UE llevará a cabo periódicamente visitas de seguimiento con objeto de comprobar que las disposiciones establecidas siguen respetando las normas mínimas acordadas.

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 Información Clasificada que podrá ser intercambiada en papel o por medios electrónicos, en particular, como consecuencia de posibles visitas de evaluación ulteriores.

4. ACUERDOS ADMINISTRATIVOS

Cuando exista la necesidad de intercambiar durante largo tiempo Información Clasificada, en principio, de un grado no superior a DIFUSÓN LIMITADA 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 con las autoridades competentes del tercer Estado o la organización internacional.

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

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

Antes de ceder efectivamente Información Clasificada al tercer Estado o la organización internacional de que se trate, se realizará una visita de evaluación con arreglo a lo dicho anteriormente y se remitirá el correspondiente informe al Comité de Seguridad, que deberá considerarlo satisfactorio. No obstante, cuando existan razones excepcionales para el intercambio urgente de Información Clasificada de las que haya sido informado el Consejo de Europa, podrá cederse la Información Clasificada, siempre que se ponga la mayor diligencia en realizar la visita de evaluación cuanto antes.

No se intercambiará Información Clasificada por medios electrónicos a menos que se haya establecido explícitamente en el acuerdo administrativo.

5. INTERCAMBIO DE INFORMACIÓN CLASIFICADA EN EL CONTEXTO DE LAS OPERACIONES PCSD[18]

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 Información Clasificada generada con motivo de operaciones PCSD a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar Información Clasificada de grado superior a DIFUSIÓN LIMITADA para operaciones civiles PCSD y CONFIDENCIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

Los acuerdos de participación ad hoc celebrados para una operación PCSD específica incluirán disposiciones sobre la cesión de Información Clasificada generada a efectos de dicha operación a terceros Estados u organizaciones internacionales contribuyentes. No se podrá intercambiar Información Clasificada de grado superior a DIFUSIÓN LIMITADA para operaciones civiles PCSD y CONFIDENCIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

Los acuerdos administrativos ad hoc sobre la participación de un tercer Estado o una organización internacional en una operación PCSD específica podrán incluir, entre otras cosas, la cesión de Información Clasificada generada a efectos de la operación a dicho tercer Estado u organización internacional. Dichos acuerdos administrativos ad hoc se celebrarán de conformidad con los procedimientos establecidos en los puntos anteriores. No se podrá intercambiar Información Clasificada de grado superior a DIFUSIÓN LIMITADA para operaciones civiles PCSD y CONFIDENCIAL para operaciones militares PCSD, a menos que se prescriba otra cosa en la decisión que establezca cada operación PCSD.

No será preciso establecer disposiciones de aplicación ni efectuar visitas de evaluación antes de aplicar las disposiciones en materia de cesión de Información Clasificada en el contexto de los puntos anteriores.

Cuando el Estado anfitrión en cuyo territorio se lleve a cabo una operación PCSD no tenga con la UE ningún acuerdo o acuerdo administrativo de seguridad de la información en vigor para el intercambio de Información Clasificada, podrá celebrarse un acuerdo administrativo ad hoc en caso de necesidad operativa específica e inmediata. Esta posibilidad se dispondrá en la decisión que establezca la operación PCSD. La Información Clasificada 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 DFUSIÓN LIMITADA. En el marco del citado acuerdo administrativo ad hoc, el Estado anfitrión se comprometerá a proteger la Información Clasificada conforme a estándares mínimos no menos estrictos que los establecidos por la presente Decisión 2011/292/UE.

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 anteriores establecerán que el tercer Estado u organización internacional afectado deberá garantizar que su personal destinado en comisión de servicio a la operación protegerá la Información Clasificada con arreglo a las normas de seguridad del

[18] Una operación militar o civil de gestión de crisis en virtud del título V, capítulo 2, del Tratado de la UE.

Consejo y con cualquier otra directriz emitida por las autoridades competentes, incluida la cadena de mando de la operación.

Si la UE y el tercer Estado o la organización internacional contribuyente celebran ulteriormente un acuerdo de seguridad de la información, este acuerdo sustituirá a 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 Información Clasificada.

No se permitirá el intercambio de Información Clasificada 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.

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

6. CESIÓN *AD HOC* CON CARÁCTER EXCEPCIONAL DE INFORMACIÓN CLASIFICADA

En caso de que no exista un marco de conformidad con los epígrafes 3, 4 y 5, y cuando el Consejo o uno de sus órganos preparatorios determine que es necesario, a título excepcional, ceder Información Clasificada a un tercer Estado o a una organización internacional, la Secretaría General del Consejo de la UE:

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 Información Clasificada que se les ceda será protegida con arreglo a estándares no menos estrictos que los establecidos por la presente Decisión.
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 Información Clasificada.

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

Si la recomendación del Comité de Seguridad no es favorable a la cesión de la Información Clasificada:

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.

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.

Una vez que se haya tomado la decisión de ceder Información Clasificada, la Secretaría General del Consejo de la UE 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 Información Clasificada que reciba de acuerdo con los principios básicos y las normas mínimas que se establecen en la Decisión 2011/292/UE.

7. AUTORIDAD PARA CEDER INFORMACIÓN CLASIFICADA A TERCEROS ESTADOS U ORGANIZACIONES INTERNACIONALES

Cuando exista un marco para el intercambio de Información Clasificada con un tercer Estado u organización internacional, el Consejo adoptará una decisión que autorice al Secretario General a ceder Información Clasificada al tercer Estado o la organización internacional de que se trate, respetando el principio del consentimiento previo del originador.

Cuando exista un marco para el intercambio de Información Clasificada con un tercer Estado u organización internacional, se autorizará al Secretario General a ceder Información Clasificada, de conformidad con la decisión por la que se establezca la operación PCSD y respetando el principio del consentimiento previo del originador.

El Secretario General podrá delegar las citadas autorizaciones en altos funcionarios de la Secretaría General del Consejo de la UE u otras personas bajo su autoridad.

ANEXO VIII

DEFINICIONES DE TÉRMINOS USADOS EN EL PRESENTE PROCEDIMIENTO[19]

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.
Amenaza	La posible causa de un incidente no deseado que pueda ocasionar daños a una organización o a alguno de los sistemas que use. Las amenazas pueden ser accidentales o deliberadas (maliciosas) y constan de elementos amenazadores, posibles blancos y métodos de ataque.
Autoridad de Seguridad Designada (ASD)	La autoridad responsable ante la Autoridad Nacional de Seguridad (ANS) de un Estado miembro, encargado de ceder 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.
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 una HPS nacional o de la UE válida, y que indica el grado de Información Clasificada a que puede tener acceso (CONFIDENCIAL o superior), el período de validez de la habilitación y la fecha de caducidad del propio certificado.
Ciclo de vida de un Sistema de Información	La duración completa de la existencia de un Sistema de Información, que comprende inicio, concepción, planificación, análisis de requisitos, diseño, desarrollo, pruebas, aplicación, funcionamiento y mantenimiento, y desmantelamiento.
Cláusula sobre	Conjunto de condiciones contractuales especiales impuestas

[19] Atendiendo a lo dispuesto en la Decisión 2011/292/UE, de 31 de marzo, sobre las normas de seguridad para la protección de la información clasificada en la UE.

aspectos de la seguridad	por la autoridad contratante y que forman parte integrante de un contrato clasificado que conlleve el acceso a Información Clasificada o la creación ese tipo de información. En ella se enumeran los requisitos de seguridad o los elementos del contrato que requieren protección de seguridad.
Contratista	La persona física o jurídica con capacidad legal para celebrar contratos.
Contrato Clasificado	El contrato celebrado entre una autoridad pública de la UE o de sus Estados miembros 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 Información Clasificada o la creación de dicha información.
Defensa en profundidad	La aplicación de una serie de medidas de seguridad organizadas a modo de defensa en barreras sucesivas.
Desclasificación	Supresión de toda clasificación de seguridad.
Documento	Toda información registrada, independientemente de su soporte o características físicas.
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.
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 Información Clasificada de un grado específico de clasificación de seguridad, y de que el personal que trabaja en dicho establecimiento y necesita acceder a Información Clasificada ha sido debidamente habilitado y ha sido formado sobre los requisitos de seguridad necesarios para acceder a la Información Clasificada y para protegerla.
Habilitación Personal de Seguridad de la UE (HPS UE)	Para acceder a Información Clasificada. La autorización que dimana de la autoridad facultada para proceder a los nombramientos de la Secretaría General del Consejo de la UE, otorgada de conformidad con la Decisión 2011/292/UE una vez realizada una investigación de seguridad por parte de las autoridades competentes de un

	Estado miembro, mediante la cual se acredita que una persona puede tener acceso a Información Clasificada de un determinado grado (CONFIDENCIAL o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información; de la persona que se ajuste a esta descripción se dirá que está "habilitada".
Habilitación Personal de Seguridad nacional (HPS nacional)	Para acceder a Información Clasificada. 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 Información Clasificada de un determinado grado (CONFIDENCIAL o superior) hasta una fecha determinada, siempre que se establezca su necesidad de conocer dicha información; de la persona que se ajuste a esta descripción se dirá que está "habilitada".
Información Clasificada de la UE	Información Clasificada. Véase texto del Procedimiento.
Inscripción en un registro	Véase el Anexo IV.
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.
Interconexión	Véase el anexo V.
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 nacional o de la UE para acceder a Información Clasificada de un determinado grado (CONFIDENCIAL o superior).
Manejo	De Información Clasificada. Toda intervención posible a la que puede estar sujeta a lo largo de su ciclo de vida la Información Clasificada, es decir: producción, tratamiento, traslado, reducción del grado de clasificación, desclasificación y destrucción. En relación con los Sistemas de Información abarca asimismo su recopilación, exposición, transmisión y almacenamiento.
Material	Todo documento, máquina o aparato, producido o en proceso

	de producción.
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.
Modo de operación de seguridad	El conjunto de las condiciones de funcionamiento de un Sistema de Información, 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 Sistema de Información 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 Sistema de Información. • "Modo unificado a nivel superior": modo de operación en el que todas las personas con acceso al Sistema de Información 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 Sistema de Información 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 Sistema de Información están habilitadas al grado más alto de clasificación de la información manejada en él, pero no todas las personas con acceso al Sistema de Información 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 Sistema de Información están habilitadas al grado más alto de clasificación de la información manejada en él, y no todas las personas con acceso al Sistema de Información tienen la misma necesidad de conocer la información manejada en él.
Operación PCSD	Una operación militar o civil de gestión de crisis en virtud del título V, capítulo 2, del Tratado de la UE.

Originador	La institución, agencia, órgano u organismo de la UE, del Estado miembro, del tercer Estado o de la organización internacional bajo cuya autoridad se ha producido Información Clasificada o se ha introducido en las estructuras de la UE.
Poseedor	Persona debidamente autorizada con una probada "Necesidad de Conocer" la información, que está en posesión de cualquier Información Clasificada y es, por tanto, responsable de su protección.
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.
Reducción del grado de clasificación	Reducción del grado de clasificación de seguridad.
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 Sistemas de Información, 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.
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.
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 personas que trabajen por cuenta propia.
Subcontrato clasificado	El contrato celebrado por un contratista de alguna de las instituciones u organismos de la UE o de sus Estados miembro o con cualquier 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 Información Clasificada o la creación de dicha información.
TEMPEST	La investigación, estudio y control de las emanaciones electromagnéticas comprometedoras y las medidas para suprimirlas.
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.