V. — OTRAS DISPOSICIONES

NORMAS

Resolución 320/14546/13, de 23 de septiembre, del Director General de Armamento y Material, por la que se aprueban los procedimientos para la implementación de la Instrucción 52/2013, de 17 de junio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la seguridad de la información del Ministerio de Defensa en poder de las empresas.

La disposición final primera de la Instrucción 52/2013, de 17 de junio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la Seguridad de la Información del Ministerio de Defensa faculta al Director General de Armamento y Material para desarrollar la normativa de tercer nivel sobre seguridad de la información en poder de las empresas.

En su virtud, resuelvo:

Primero.- Aprobar los Procedimientos, relativos a la protección de la información clasificada del Ministerio de Defensa en poder de las empresas, en virtud de su participación en proyectos, contratos o programas promovidos por el mismo cuyo texto se incluye en las direcciones web que se indican en el apartado cuarto.

Dichos procedimientos recogen lo relativo a:

- Obtención, modificación del grado, suspensión o retirada de la Habilitación de Seguridad de Empresa (HSEM) y, en su caso, la Habilitación de Seguridad de Establecimiento (HSES) necesarias para que las empresas puedan participar en los contratos en los que se maneje información clasificada. Estas habilitaciones son las exigidas por la Ley 24/2001, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y la seguridad.
- Obtención de la Habilitación Personal de Seguridad (HPS), por parte de todas aquellas personas de las empresas que tengan necesidad de acceder a información clasificada de Programas Proyectos o Contratos Clasificados del MINISDEF.
- Apertura y cierre del/los Órgano/s de Control que deben disponer las empresas para el manejo de la información clasificada.
- Tratamiento de la información clasificada (acceso, distribución, reproducción, traducción, destrucción, etc.).
- Comunicación y autorización de visitas en las que se vaya a acceder a información clasificada, así como los planes de transporte que afecten a este tipo de información.
- Acreditación de los sistemas CIS con los que las empresas vayan a manejar información clasificada.

Segundo.- El ámbito de aplicación de estos Procedimientos comprende a todo el Ministerio de Defensa y a todas las empresas que manejen o puedan manejar información del MINISDEF.

Tercero.- El objeto de esta Resolución es el desarrollo normativo de tercer nivel sobre seguridad de la información en poder de las empresas, de acuerdo con lo dispuesto en la Instrucción 52/2013, de 17 de junio de 2013, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información del Ministerio de Defensa (MINISDEF) en poder de las empresas.

Cuarto.- La presente Resolución junto con los Procedimientos podrá ser consultada y descargada en las siguientes direcciones url:

INTRANET:

http://portal.mdef.es/WEBDGAM/servicios tecnicos acuerdos.htm

INTERNET:

http://www.defensa.gob.es/info/servicios/servicios-tecnicos/SEGINFOEMP/

CVE: BOD-2013-208-24581

En estas direcciones estarán también disponibles los formularios a que hacen referencia los Procedimientos.

Quinto.- La presente Resolución entrará en vigor al día siguiente de su publicación en el «Boletín Oficial de Defensa».

Madrid, 23 de septiembre de 2013.—El Director General de Armamento y Material, Juan Manuel García Montaño.

CVE: BOD-2013-208-24582

DESARROLLO NORMATIVO DE TERCER NIVEL

PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE LA INSTRUCCIÓN 52/2013, DE 17 DE JUNIO, DEL SECRETARIO DE ESTADO DE DEFENSA, POR LA QUE SE APRUEBAN LAS NORMAS PARA LA SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DEFENSA EN PODER DE LAS EMPRESAS

ÍNDICE

Pág.

1. INTRODUCCIÓN

La Disposición final primera de la Instrucción 52/2013 del Secretario de Estado de Defensa, por la que se aprueban las normas para la Seguridad de la Información del Ministerio de Defensa faculta al Director General de Armamento y Material para desarrollar la normativa de tercer nivel sobre seguridad de la información en poder de las empresas.

En consecuencia, se aprueban los siguientes procedimientos relativos a la protección de la información clasificada del Ministerio de Defensa en poder de las empresas, en virtud de su participación en proyectos, contratos o programas promovidos por el mismo.

Dichos procedimientos recogen lo relativo a:

- Obtención, modificación del grado, suspensión o retirada de la Habilitación de Seguridad de Empresa (HSEM) y, en su caso, la Habilitación de Seguridad de Establecimiento (HSES) necesarias para que las empresas puedan participar en los contratos en los que se maneje información clasificada. Estas habilitaciones son las exigidas por la Ley 24/2001, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y la seguridad.
- Obtención de la Habilitación Personal de Seguridad (HPS), por parte de todas aquellas personas de las empresas que tengan necesidad de acceder a información clasificada de Programas Proyectos o Contratos Clasificados del MINISDEF.
- Apertura y cierre del/los Órgano/s de Control que deben disponer las empresas para el manejo de la información clasificada.
- Tratamiento de la información clasificada (acceso, distribución, reproducción, traducción, destrucción, etc.).
- Comunicación y autorización de visitas en las que se vaya a acceder a información clasificada, así como los planes de transporte que afecten a este tipo de información.
- Acreditación de los sistemas CIS con los que las empresas vayan a manejar información clasificada.

Por último, se ha añadido un breve glosario de términos y definiciones y un conjunto de anexos en el que se recogen distintos formularios y documentos a emplear en relación con los procedimientos.

2. OBJETO

De acuerdo con lo dispuesto en la Instrucción 52/2013, de 17 de junio de 2013, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información del Ministerio de Defensa (MINISDEF) en poder de las empresas, el objeto de esta Resolución es el desarrollo normativo de tercer nivel sobre seguridad de la información en poder de las empresas.

3. ÁMBITO DE APLICACIÓN

Estos procedimientos afectan a todo el departamento y serán de aplicación a todas las empresas que manejen o puedan manejar información del MINISDEF.

4. HABILITACIÓN DE SEGURIDAD DE EMPRESA (HSEM)

4.1. Procedimiento para la obtención de HSEM

Para participar en programas, proyectos o contratos clasificados del Ministerio de Defensa, en el que se vaya a manejar información clasificada de grado "CONFIDENCIAL" o superior, las empresas contratistas necesitan disponer de una HSEM del grado adecuado a la clasificación del programa, proyecto o contrato, que las faculta para generar y acceder a información clasificada, sin que pueda manejarla o almacenarla en sus propias instalaciones.

En el caso de que el contrato, programa o proyecto se hay clasificado de grado "DIFUSIÓN LIMITADA", el contratista debería estar en posesión de HSEM de grado CONFIDENCIAL, que es la de menor grado que se concede.

Para obtenerla, deberá solicitarla a la Dirección General de Armamento y Material (DGAM).

Además de la HSEM, toda empresa deberá constituir, como Órgano de Control, un Servicio de Protección de Materias Clasificadas (SPMC), integrado por uno o varios Servicios Locales de Protección de Materias Clasificadas (SLPMC) o, si fuese necesario, un Servicio General de Protección de Materias Clasificadas (SGPMC).

Dependiendo de que se trate de personas jurídicas o físicas, el procedimiento a seguir para solicitar la HSEM y la apertura del Órgano de Control será el siguiente:

4.1.1. Personas jurídicas

Se presentará por escrito solicitud firmada por el responsable máximo de la empresa o apoderado de la misma dirigido a la DGAM (Subdirección General de Inspección y Servicios Técnicos, en adelante SDG INSERT).

En el escrito se indicará claramente que se solicita una HSEM y la apertura de un SLPMC o SGPMC. A este escrito se unirá la siguiente documentación:

a) Documento acreditativo, suscrito por un Organismo del Ministerio de Defensa relacionado con el programa, proyecto o contrato clasificado, que justifique la viabilidad/necesidad de que el contratista pueda participar en dicho programa, proyecto o contrato, que implique acceso a información clasificada. (Ver anexo I).

b) Solicitud de Habilitación Personal de Seguridad (HPS) de las personas elegidas por el contratista para el desempeño del cargo de Jefe de Seguridad del Servicio de Protección (JSSP) y del suplente de dicho JSSP, así como del Jefe de Seguridad del Órgano de Control y de su suplente, cuando no sean los anteriores. (Ver formularios del anexo II).

c) Solicitud de HPS del grado que corresponda de las personas que inicialmente vayan a acceder a información clasificada, empleando los mismos formularios del apartado b).

d) Solicitud de HPS de los propietarios, administradores (ya sean únicos, solidarios o mancomunados), de los miembros del consejo de administración y de cualquier otra persona que pueda conocer, participar o estar presente en las

deliberaciones del órgano ejecutivo del contratista. En su caso, la solicitud de HPS de estas personas podrá ser sustituida por un acta notarial de renuncia al acceso a información clasificada. Se emplearán también los formularios del apartado b) y, en caso de presentar acta notarial de renuncia, se hará según el texto contenido en el anexo III.

e) Copia del poder notarial, o fotocopia compulsada, que autorice a la persona designada por el contratista para firmar el Compromiso de Seguridad (Ver anexo 0). Si dicha persona no dispone de poderes generales en la empresa, habrá de obtener un poder específico en el que figure el texto del anexo IV.

f) Copia simple notarial, o fotocopia compulsada, de la escritura de constitución de la sociedad, así como documentación acreditativa de las ampliaciones o variaciones sufridas posteriormente, tanto propias como de aquellas sociedades que participen en la solicitante, o sean participadas de ella.

g) Certificado de inscripción en el Registro Mercantil, caso de no estar reflejada en las escrituras especificadas en el punto anterior.

h) Última declaración completa del Impuesto de Sociedades.

i) Memoria del contratista que abarque los aspectos que expliquen su experiencia y capacidad profesional, así como las referencias que estime oportunas.

j) "Ficha del contratista", según formato establecido en el anexo V.

k) Certificado de la Agencia Estatal de Administración Tributaria u organismo autonómico equivalente, de que se encuentra al corriente de pago de sus obligaciones tributarias, emitido como máximo tres meses antes de la presentación de la documentación.

l) Certificado emitido por la Tesorería de la Seguridad Social de que se encuentra al corriente de sus obligaciones, emitido como máximo tres meses antes de la presentación de la documentación.

m) En el caso de las empresas de seguridad privada:

- Certificado vigente de Inscripción en el Registro General de Empresas de Seguridad del Ministerio del Interior, conforme al Artículo 7 de la Ley 23/1992 de 30 de Julio de Seguridad Privada y las modificaciones posteriores del mismo. Quedan exentas de dicho ámbito las empresas ubicadas únicamente en Ceuta, Melilla o en territorios insulares.

- Certificado del Ministerio del Interior que atestigüe las sanciones que se hayan incoado a la empresa, conforme a la Sección Segunda del Capítulo cuarto de la Ley 23/1992 de 30 de Julio de Seguridad Privada, en los diez años previos a la solicitud del Compromiso de Seguridad.

n) Cualquier otra que le sea solicitada por ser necesaria para determinar que cumple los requisitos para la concesión de la HSEM.

Si del examen de la documentación se deduce que se puede conceder la HSEM a la empresa, la Autoridad competente la citará para que la persona designada firme el "Compromiso de Seguridad" y le será comunicada la concesión mediante escrito oficial en el que se indicará el grado de la misma, así como la apertura del SLPMC o SGPMC solicitado.

Las HSEM podrán ser de uno de los siguientes grados: SECRETO, RESERVADO y CONFIDENCIAL.

El Compromiso de Seguridad representa la obligación que asume voluntariamente el contratista ante la Administración para el exacto cumplimiento de las disposiciones relativas a la protección de la información clasificada (de grado "CONFIDENCIAL" o Superior).

En virtud del Compromiso de Seguridad, el contratista se obliga formalmente, a proteger la información clasificada que genere, maneje o almacene, en razón de la ejecución de una actividad, contrato o programa clasificado de grado "CONFIDENCIAL" o Superior, conforme a los requisitos exigidos por la normativa de protección de la información clasificada en vigor, así como a recibir inspecciones periódicas y a devolver la información clasificada cuando le sea requerida.

Se significa que la obtención de HSEM y la apertura de un Órgano de Control no capacitan, por sí mismos, a la empresa para almacenar información clasificada en sus instalaciones, excepto la correspondiente a las Habilitaciones Personales de Seguridad que haya solicitado. Para poder almacenar información clasificada en sus instalaciones, deberá solicitar, además, una HSES, según el procedimiento descrito posteriormente.

4.1.2. Personas físicas.

a) Documento acreditativo, suscrito por un Organismo del Ministerio de Defensa relacionado con el programa, proyecto o contrato clasificado, que justifique la viabilidad/necesidad de que el contratista pueda participar en dicho programa, proyecto o contrato que implique acceso a información clasificada. (Ver anexo I).

b) Solicitud de Habilitación Personal de Seguridad (HPS) de las personas elegidas por el contratista para el desempeño del cargo de Jefe de Seguridad del Servicio de Protección (JSSP) y del suplente de dicho JSSP, así como del Jefe de Seguridad del Órgano de Control y de su suplente, cuando no sean los anteriores. Para ello se emplearán los formularios que se encuentran en el anexo II.

c) Solicitud de HPS del grado que corresponda de las personas que inicialmente vayan a acceder a información clasificada, empleando los mismos formularios del apartado b).

d) Solicitud de HPS o renuncia notarial de las personas que tuviera contratadas consideradas como "vinculadas", es decir, familiares hasta segundo grado incluido (abuelos, padres, cónyuges, hijos, nietos o hermanos). En su caso, la solicitud de HPS de estas personas podrá ser sustituida por un acta notarial de renuncia al acceso a información clasificada. (Ver anexo III).

e) Copia del poder notarial, o fotocopia compulsada, que autorice a la persona designada por el contratista para firmar el Compromiso de Seguridad (anexo 0), cuando no sea la propia persona física que solicita la HSEM. (Ver anexo IV).

f) Declaración Censal (modelos 036 ó 037) presentado en la Agencia Tributaria cuando se inicia, se modifica o se da de baja una actividad económica, acreditativa de la inscripción en el Censo de empresarios, profesionales y retenedores, con identificación de la actividad, los regímenes y obligaciones tributarias del IRPF e IVA, así como el domicilio.

g) Última declaración del IRPF y, en su caso, del Impuesto sobre el Patrimonio, acompañada de los siguientes documentos:

- Central de Información de Riesgos del Banco de España (CIRBE) y Certificado Bancario de Solvencia emitido por el banco o bancos con los que tenga una mayor relación comercial.
- Modelo 190: Retenciones de IRPF efectuadas a sus trabajadores.
- Modelo 347: Declaración de operaciones con terceros. Compras o ventas superiores a 3.005'06 €.

h) Memoria del contratista que abarque los aspectos que expliquen su experiencia y capacidad profesional, así como las referencias que estime oportunas.

i) "Ficha del contratista", según formato establecido en el anexo V.

j) Certificado de la Agencia Estatal de Administración Tributaria correspondiente u organismo autonómico equivalente, de que se encuentra al corriente de pago de sus obligaciones tributarias, emitido como máximo tres meses antes de la presentación de la documentación.

k) Certificado emitido por la Tesorería de la Seguridad Social de que se encuentra al corriente de sus obligaciones, emitido como máximo tres meses antes de la presentación de la documentación.

l) Cualquier otra que le sea solicitada por ser necesaria para determinar que cumple los requisitos para la concesión de la HSEM.

Si del examen de la documentación se deduce que se puede conceder la HSEM a la empresa, la Autoridad competente la citará para que la persona designada firme el "Compromiso de Seguridad" y le será comunicada la concesión mediante escrito oficial en el que se indicará el grado de la misma, así como la apertura del SLPMC o SGPMC solicitado.

Las HSEM podrán ser de uno de los siguientes grados: SECRETO, RESERVADO y CONFIDENCIAL.

El Compromiso de Seguridad representa la obligación que asume voluntariamente el contratista ante la Administración para el exacto cumplimiento de las disposiciones relativas a la protección de la información clasificada.

En virtud del Compromiso de Seguridad, el contratista se obliga formalmente, a proteger la información clasificada que genere, maneje o almacene en razón de la ejecución de una actividad, contrato o programa clasificado de grado "CONFIDENCIAL" o Superior, conforme a los requisitos exigidos por la normativa de protección de la información clasificada en vigor, así como a recibir inspecciones periódicas y a devolver la información clasificada cuando le sea requerida.

Se significa que la obtención de HSEM y la apertura de un Órgano de Control no capacitan, por sí mismos, a la empresa para almacenar información clasificada en sus instalaciones, excepto la correspondiente a las Habilitaciones Personales de Seguridad que haya solicitado. Para poder almacenar información clasificada en sus instalaciones, deberá solicitar, además, una Habilitación de Seguridad de Establecimiento (HSES), según el procedimiento descrito posteriormente.

4.2. Procedimiento para la modificación de la HSEM

4.2.1. Elevación del grado de la HSEM

Cuando el contratista necesite elevar el grado de la HSEM de que disponga, lo solicitará por escrito a la DGAM (SDGINSERT), acompañado de la siguiente documentación:

a) Documento de un órgano del Ministerio de Defensa, responsable del contrato, justificando la conveniencia de que el contratista participe en un contrato que implique acceso a información clasificada de mayor grado al de la HSEM vigente. (Ver anexo I).

b) Solicitud de HPS de las personas elegidas por el contratista para el desempeño del cargo de JSSP y de su suplente y, en su caso, del Jefe de Seguridad del Órgano de Control y su suplente, si estos fuesen distintos a los anteriores, con indicación del nuevo grado.

c) Solicitud de HPS de las personas que inicialmente vayan a acceder a información clasificada, correspondiente al nuevo grado.

d) Solicitud de HPS, conforme al nuevo grado, de los administradores sociales y personal directivo. En su caso, la HPS de las personas antes mencionadas podrá ser sustituida por un acta notarial de renuncia al conocimiento de información clasificada.

e) Cualquiera otra documentación que le fuera requerida con el fin de verificar que se satisfacen los criterios de estabilidad económica y fiabilidad.

(Los formularios a emplear para solicitar las HPS son los que figuran en el anexo II).

4.2.2. Reducción del grado de la HSEM

Cuando el contratista desee la reducción de grado de la HSEM, deberá solicitarlo por escrito a la DGAM (SDGINSERT).

Una vez concedida la reducción del grado solicitada, el contratista deberá entregar toda la información clasificada de grado superior al nuevo solicitado, que obrara en su poder, al Órgano que se la hubiera entregado.

4.3. Procedimiento para la suspensión de la HSEM

La HSEM podrá quedar en suspenso temporalmente cuando se determine por la Autoridad competente que las condiciones de seguridad del contratista son inadecuadas para garantizar la protección de la información clasificada, o concurran circunstancias que aconsejen su revisión.

Al serle comunicada la suspensión temporal, el contratista deberá devolver la información clasificada al Órgano de Control de información clasificada que se la hubiera entregado.

Esta situación se mantendrá mientras permanezcan las circunstancias que la motivaron y durante un plazo máximo de un año. Transcurrido el período máximo de suspensión sin que el contratista haya corregido las deficiencias que dieron lugar a la misma, se procederá a la retirada.

La suspensión temporal de la HSEM supondrá la suspensión temporal automática de las HSES que tuviera el contratista, así como la suspensión temporal automática del Órgano de Control que tuviese establecido.

4.4. Procedimiento para la retirada de la HSEM

La HSEM será retirada cuando concurra alguna de las siguientes circunstancias:

a) El contratista deje de cumplir alguno de los requisitos solicitados para la concesión de la HSEM.

b) Renuncia escrita del contratista.

c) Incumplimiento de las obligaciones adquiridas por el contratista con la firma del Compromiso de Seguridad.

d) El contratista no haya optado a ningún Contrato Clasificado durante un período de tres años consecutivos.

e) Haya transcurrido más de un año de suspensión temporal sin que el contratista haya subsanado las deficiencias encontradas.

f) Lo exija el interés o la seguridad del Estado.

Si la retirada se produce en virtud de lo señalado en c) y e), el contratista no podrá optar a una nueva HSEM hasta pasados tres (3) años desde la fecha de retirada de la HSEM anterior.

La retirada de la HSEM supondrá la retirada automática de todas las HSES que tuviera concedidas el contratista y de los Órganos de Control que tuviese establecidos, así como la suspensión de las HPS de sus empleados. El contratista devolverá la información clasificada que posea a los Órganos de Control de los que la hubiera recibido, y devolverá a la DGAM (SDG INSERT), para que ésta a su vez los remita a la Autoridad emisora, los certificados o comunicaciones de concesión de HPS de sus empleados y los certificados de acreditación de las ZAR.

4.5. Supuestos particulares

4.5.1. Unión Temporal de Empresas.

Cuando una Unión Temporal de Empresas (UTE) vaya a presentar oferta a un contrato que requiera acceso a Información clasificada, se precisará que alguna de las empresas participantes en la UTE tenga la correspondiente HSEM.

Una vez adjudicado el contrato, todas aquellas empresas de la UTE que vayan a manejar información clasificada en sus instalaciones necesitarán disponer de la HSEM, HSES y el Servicio Local o General de Protección (SLPMC/SGPMC) correspondientes.

Todo el personal de las empresas constitutivas de la UTE que precise acceder a Información clasificada deberá estar en posesión de una HPS, del grado correspondiente. El personal de aquellas empresas que forman la UTE que no dispongan de HSEM podrá solicitar HPS a través del Jefe del Servicio de Protección (JSSP) de alguna otra de las empresas de la UTE que sí estén en posesión de ella. En todo caso regirá el principio de que sólo se podrá acceder a Información clasificada en aquellos locales habilitados al efecto como Zona de Acceso Restringido (ZAR).

4.5.2. Grupo Empresarial

Para crear una estructura de seguridad de Grupo empresarial será necesario que un único apoderado represente a todas las empresas que vayan a formar parte de dicho Grupo empresarial, debiendo disponer de poderes suficientes, concedidos ante notario, de todas y cada una de las empresas del Grupo.

El contratista que pertenezca a un Grupo Empresarial deberá acreditar que las condiciones requeridas para la concesión de la HSEM no se ven afectadas por su pertenencia al Grupo empresarial.

Cuando el Grupo disponga de más de una empresa con HSEM, se podrá solicitar la designación de un Director de Seguridad del Servicio de Protección del Grupo (DSSG). En tal caso, la empresa matriz del Grupo deberá presentar la correspondiente solicitud, acompañada de la Propuesta de Personal (formulario PP-103, anexo II).

4.5.3. Subcontratistas

El JSSP del contratista, antes de iniciar las negociaciones para suscribir subcontratos que impliquen el acceso a Información clasificada, deberá solicitar:

a) La autorización expresa por escrito del órgano de contratación competente.

b) Documento acreditativo de que el subcontratista con el que se pretende iniciar la negociación dispone de las habilitaciones necesarias para acceder, almacenar o manejar la Información clasificada relativa al contrato o subcontrato. Esta certificación la podrá solicitar a la DGAM (SDGINSERT) que, en su caso, expedirá el Certificado del anexo VI.

En la solicitud de autorización, el contratista comunicará los datos de identificación del subcontratista, así como detalles sobre el mayor grado de clasificación, naturaleza y volumen de la información que éste vaya a manejar, y una explicación de la necesidad de que reciba la información. Una vez autorizado por el Órgano de Contratación, al formalizar el contrato o subcontrato, el contratista deberá comunicar al subcontratista información sobre el mayor grado de clasificación, naturaleza y volumen de la información que éste vaya a manejar.

El contratista es el responsable de solicitar la autorización de acceso a Información clasificada del personal del subcontratista. Para ello empleará el formulario del anexo VIII. Será igualmente responsabilidad del contratista informar a la DGAM (SDGINSERT) de toda incidencia que haya podido poner en riesgo la Información clasificada a la que haya accedido el subcontratista.

El subcontratista se relacionará con la DGAM (SDGINSERT) para todas las gestiones relativas a la concesión de HSEM, HSES y HPS.

Al término del contrato, el subcontratista devolverá al contratista toda la Información clasificada que obre en su poder relativa al Contrato Clasificado.

4.5.4. Empresas de Servicios

Como norma general, las empresas de servicios y de consultoría no necesitan HSEM, salvo que en ejercicio de sus funciones deban manejar Información clasificada.

El personal de estas empresas que, para el ejercicio de sus funciones, no precise el acceso a Información clasificada, aunque deba acceder a una ZAR configurada como Área de Seguridad Clase II, no necesitará disponer de HPS, pero deberá estar escoltado permanentemente.

Cuando el personal de estas empresas acceda a una ZAR configurada como Área de Seguridad Clase I, el Órgano de Control del que dependa la ZAR tendrá en cuenta que:

a) Dicho personal será siempre el mismo y su número se reducirá al mínimo posible.

b) El responsable del Órgano de Control del que dependa la ZAR deberá tramitar las solicitudes de HPS de dicho personal, según lo dispuesto en el procedimiento correspondiente.

c) Dicho personal no podrá acceder ni permanecer en la ZAR sin escolta.

Las empresas de servicios que para llevar a cabo su labor deban extraer Información clasificada de las instalaciones de una empresa que desarrolla actividades o contratos clasificados, deberán disponer de HSEM, HSES, tener establecido un Órgano de Control y los empleados que accedan a la misma deberán estar habilitados.

4.5.5. Empresas de Seguridad

Las empresas de seguridad que presten servicios de vigilancia a ZAR de empresas o instalaciones oficiales y no necesiten manejar Información clasificada en sus propias instalaciones, deberán disponer de HSEM en grado CONFIDENCIAL.

El personal de empresas de seguridad que presten servicio de vigilancia en una ZAR deberá tener HPS de grado igual o superior al de la ZAR a la que prestan servicio, permitiéndose en estos casos que se cursen solicitudes de Habilitaciones Personales de Seguridad para el personal de las empresas de seguridad de grado superior al de la HSEM.

Las empresas de seguridad que prestan servicios como instaladoras de sistemas de seguridad en ZAR de empresas o instalaciones oficiales, deberán disponer de HSEM en grado RESERVADO.

4.6. Vigencia de la HSEM

La HSEM no tiene caducidad, pero será controlada en todo momento por la Autoridad que la concedió.

5. HABILITACIÓN DE SEGURIDAD DE ESTABLECIMIENTO (HSES)

Para poder manejar y almacenar Información clasificada hasta un determinado grado en las instalaciones del contratista acreditadas para ello, será necesario disponer de Habilitación de Seguridad de Establecimiento (HSES).

5.1. Procedimiento para la obtención de Habilitación de Seguridad de Establecimiento (HSES)

El contratista podrá solicitar la HSES al mismo tiempo que la HSEM o hacerlo posteriormente de haber obtenido ésta.

El solicitante deberá presentar a la DGAM (SDGINSERT) un escrito/carta de solicitud de HSES, acompañado de la siguiente documentación:

a) Plan de Protección de la/s Zona/s de Acceso Restringido (ZAR) solicitada/s.

b) Cualquier otra que le sea solicitada, por ser necesaria para determinar que cumple los requisitos de seguridad para manejar información clasificada en sus instalaciones.

Esta documentación acompañará a la correspondiente a la solicitud de HSEM, en el caso de que se hayan solicitado ambas habilitaciones de manera simultánea.

El Plan de Protección consta de:

- El Plan de Acondicionamiento.
- El Plan de Seguridad.
- El Plan de Emergencia.

A modo orientativo, para la elaboración del Plan de Protección y la constitución de la Zona de Acceso Restringido, se pueden consultar los siguientes enlaces:

Orientaciones para el Plan de Protección:

http://www.cni.es/comun/recursos/descargas/OR-ASIP-01-01_03_Orientaciones_para_el_Plan_de_Proteccion_de_una_ZAR.pdf

Orientaciones para la constitución de ZAR:

http://www.cni.es/comun/recursos/descargas/OR-ASIP-01-02_03_Orientaciones_para_la_Constitucion_de_ZAR.pdf

Se recomienda su confección en formato electrónico, para facilitar su posterior actualización. El Plan de Protección debe reflejar, en todo momento, la situación real de la seguridad de la empresa, por lo que habrá que actualizarlo cada vez que haya cambios en la misma.

Una vez elaborado y presentado el Plan de Protección, se procederá a inspeccionar la/s Zona/s de Acceso Restringido por parte de la DGAM (SDG INSERT) y, si el resultado de la inspección es satisfactorio, se expedirá un Certificado de Inspección y Cumplimiento. Si esta inspección no resulta positiva, se adoptarán las medidas correctoras necesarias para solventarlas, requiriendo una inspección y certificación posterior Una vez que la Autoridad competente conceda la HSES a una empresa, le será oficialmente comunicada por escrito, con indicación del grado que se le haya otorgado, así como su fecha de caducidad, que será la que viene reflejada en el

Certificado de Acreditación de Locales (CAL), que se le adjuntará y deberá colocar en la ZAR constituida, En este mismo escrito se le comunicará igualmente la apertura del SLPMC o SGPMC solicitado, que tendrá capacidad para almacenar Información clasificada hasta el grado concedido.

5.2. Procedimiento para la modificación del grado de la HSES

5.2.1. Elevación del grado de la HSES.

Si el contratista tiene concedida HSES de un determinado grado y necesita elevarlo, deberá presentar solicitud por escrito a la DGAM (SDGINSERT), acompañando la siguiente documentación:

a) Solicitud de elevación de grado de la HSEM según lo dispuesto en procedimiento descrito anteriormente, dado que la HSES no puede ser de grado superior al de la HSEM.

b) Solicitud de acreditación de la/s ZAR, una vez adaptada/s las medidas de seguridad al nuevo grado.

c) Solicitud de autorización de los Sistemas de Información y Comunicaciones, una vez adaptadas las medidas de seguridad al nuevo grado de clasificación, si los tuviera.

d) Plan de Protección adecuado a las nuevas medidas de seguridad y grado.

5.2.2. .Reducción del grado de la HSES.

a) Cuando el contratista desee la reducción de grado de la HSEM o HSES, deberá solicitarlo por escrito a la DGAM (SDGINSERT).

b) Una vez concedida la reducción del grado solicitada, el contratista deberá entregar toda la Información clasificada de grado superior al nuevo solicitado, que obrara en su poder, al Órgano que se la hubiera entregado.

5.3. Procedimiento para la suspensión de la HSES

La HSES podrá quedar en suspenso temporalmente cuando se determine por la Autoridad competente que las condiciones de seguridad del contratista son inadecuadas para garantizar la protección de la Información clasificada, o concurran circunstancias que aconsejen su revisión.

Al serle comunicada la suspensión temporal, el contratista deberá devolver la Información clasificada al Órgano de Control de Información clasificada que se la hubiera entregado.

Esta situación se mantendrá mientras permanezcan las circunstancias que la motivaron y durante un plazo máximo de un año. Transcurrido el período máximo de suspensión sin que el contratista haya corregido las deficiencias que dieron lugar a la misma, se procederá a la retirada.

La suspensión temporal de la HSEM supondrá la suspensión temporal automática de las HSES y la de los Órganos de Control que tuviese establecidos el contratista.

5.4. Procedimiento para la retirada de la HSES

La HSES podrá ser retirada, a petición del contratista, cuando no necesite almacenar o manejar Información clasificada en sus instalaciones, o cuando la

Autoridad competente estime que el contratista no cumple adecuadamente con las normas de seguridad establecidas.

6. HABILITACIÓN PERSONAL DE SEGURIDAD (HPS)

6.1. Procedimiento de Solicitud de HPS

El proceso para llegar a conceder una HPS se basa en una investigación sobre las condiciones de seguridad del solicitante y de su entorno, es decir, en la realización de un análisis de los riesgos presentes.

El solicitante conoce, y autoriza, que va a ser sometido a un proceso de investigación, personal y de su entorno. La investigación será tanto más exhaustiva en tanto el grado de información clasificada al que se necesite acceder sea mayor.

Para ello el sujeto debe presentar un expediente de solicitud en el que, junto al objeto de la solicitud, se aportan los datos iniciales para la realización de dicha investigación. Durante el transcurso de la misma se podrán solicitar los datos adicionales que se estimen necesarios para determinar el riesgo.

Dicha investigación ha de apoyarse en un el análisis de datos del solicitante y su entorno, que permita descartar que existan, en ese momento, vulnerabilidades o amenazas conocidas. Del resultado de dicho análisis se inferirá un grado de confianza en la lealtad, honradez, fiabilidad y vulnerabilidad de las personas a las que se conceda acceso a Información clasificada.

La capacidad de investigación no se agota una vez concedida la HPS, sino que podrá retomarse en cualquier momento durante el período de vigencia de la misma, por tratarse de un proceso de evaluación continua de las condiciones de seguridad.

El procedimiento para la solicitud de HPS será el mismo con independencia del tipo solicitado. Las variaciones en el procedimiento vendrán determinadas por el grado y la especialidad.

Estar en posesión de una HPS de un tipo concreto no garantiza, directa y necesariamente, la concesión de acceso a otros diferentes, siendo precisa para ello una nueva solicitud. No obstante, dicha posesión podrá determinar que, en casos concretos, definidos por procedimientos particulares, no sea preciso realizar investigaciones adicionales para la concesión de la HPS para los nuevos accesos solicitados.

Los grados de HPS que habilitan para el acceso a información clasificada nacional o procedente de otro país en base a un Acuerdo para la Protección de información clasificada, de mayor a menor, son los siguientes:

- SECRETO (S)
- RESERVADO (R)
- CONFIDENCIAL (C)

En el ámbito NACIONAL, existen las especialidades:

- CRIPTO: Capacita a sus titulares el acceso al conocimiento y manejo de la documentación y claves utilizadas en los equipos y sistemas criptográficos y de claves de comunicaciones nacionales, o, al amparo de un Acuerdo de Seguridad válido que así lo contemple, de otra nación.
- SIGINT: Con la misma función que la especialidad COMINT-INDOCTRINATED (del ámbito OTAN), pero en el ámbito nacional.

Con carácter general, los requisitos para poder solicitar HPS son:

a) Tener más de 18 años de edad.

b) Tener plena capacidad legal.

c) Ser español, o nacional de algún Estado miembro de la OTAN o de la UE, o nacional de algún otro Estado con el que ESPAÑA tenga establecido Acuerdo para la Protección de información clasificada, que contemple el pleno reconocimiento mutuo de la facultad para emitir HPS válidas y de la capacidad de ejecución de los procedimientos asociados.

   Se estudiará caso por caso la conveniencia o no de la concesión, al objeto de evitar que se dé un posible conflicto de lealtades.

d) El solicitante ha ostentado alguna de dichas nacionalidades durante el siguiente tiempo mínimo, inmediato al de solicitud de la HPS:

   - tres (3) años, para HPS de grado “CONFIDENCIAL”,

   - cinco (5) años, para HPS de grado “RESERVADO”, y

   - diez (10) años, para HPS de grado “SECRETO”.

e) Tratándose de casos de doble nacionalidad, en los que una de las nacionalidades del solicitante no coincida con alguna de las señaladas anteriormente, la solicitud de HPS será objeto de un análisis caso por caso, al objeto de evitar que se dé un posible conflicto de lealtades.

El personal de procedencia extranjera que no cumpla los anteriores requisitos de elegibilidad no podrá, por tanto, ser asignado a ningún puesto que implique la necesidad de estar en posesión de una HPS.

El contratista solicitará únicamente HPS para aquellos empleados que necesiten acceder a información clasificada para el desarrollo de una actividad o contrato clasificado.

Para la obtención de HPS de una persona, el responsable del Servicio de Protección de la empresa remitirá por escrito a la DGAM (SDGINSERT) solicitud acompañada del formulario HPS del anexo II, cumplimentado.

Para su correcta cumplimentación, podrá consultar la ayuda que aparece en el citado anexo II.

En caso de solicitar la HPS para varias personas, podrá enviar juntos los documentos de cada una de ellas.

El expediente de solicitud de de HPS consta de:

− Solicitud de Habilitación Personal de Seguridad, (SHPS-100),

  En este formulario, el solicitante se identifica con sus datos fundamentales y expresa lo que solicita, junto con una justificación detallada de la necesidad. Asimismo, el Jefe o responsable de quien depende, con el nivel de responsabilidad y la competencia adecuados, certificará la necesidad y la pertinencia de la solicitud.

− Declaración Personal de Seguridad, (DPS- 101).

  A rellenar por todo solicitante, sin exclusión alguna, quien certifica con su firma la veracidad de los datos aportados y que son completos. Este formulario es la base

para la investigación posterior. El cuestionario tiene un carácter progresivo, en el sentido de ser mayor el volumen de datos que han de ser aportados al aumentar el grado de habilitación solicitado.

- Propuesta de Personal, (PP-103).

En este formulario, el contratista especifica el perfil de seguridad del solicitante y los contratos clasificados en los que se prevé su participación. Incluye el visto bueno del Representante del Área de Seguridad de la información clasificada en poder de las Empresas, que avala con su firma el proceso de solicitud.

A los efectos de la solicitud de HPS, podrán ser también tramitadas por el contratista las correspondientes a:

a) Los asesores o consultores externos que acceden a información clasificada en la sede del contratista para realizar sus cometidos, y que no disponen de la HPS necesaria en su empresa u organismo de procedencia.

b) El personal de servicios (limpieza, mantenimiento) que no dispone de HPS en su empresa de procedencia y que deba acceder a una ZAR en la sede del contratista, para realizar sus cometidos.

c) Personal vinculado al contratista y no contemplado en los casos anteriores, cuyo acceso a información clasificada es necesario para el desarrollo de una Actividad o Contrato Clasificado.

En todos los casos anteriores, la solicitud irá acompañada de un informe del contratista sobre la empresa prestataria de servicios.

La solicitud de HPS para un empleado de nacionalidad extranjera, deberá acompañarse de una justificación escrita, donde el contratista especifique las razones o motivos para la participación del solicitante en la actividad, el contrato o proyecto clasificado concreto que implique el acceso a Información clasificada. Deberá además presentar una autorización escrita del organismo propietario de la información, y cumplir, en su caso, con lo establecido en las instrucciones de seguridad del programa y cláusulas de seguridad del contrato.

La Habilitación Personal de Seguridad será válida sólo en el ámbito de la empresa con HSEM para la que trabaja.

La DGAM (SDGINSERT) comunicará por escrito a la empresa la concesión de las habilitaciones que ésta haya solicitado., mediante un Listado de Comunicación de Concesión de HPS.

Las HPS concedidas y los Listados de Concesión de HPS, aunque no constituyen documentos clasificados, serán custodiadas por la DGAM (SDGINSERT), la cual mantendrá un registro actualizado de las mismas.

Cuando el titular de una HPS cambie de empresa, el JSSP de la empresa en la que ha causado baja, deberá comunicarla a la DGAM (SDG INSERT). Por su parte, si la nueva empresa precisa que dicha persona continúe habilitada, deberá presentar por escrito en la DGAM (SDGINSERT) nueva Propuesta de Personal (PP-103), significándose que para poder realizar esta solicitud, la empresa deberá disponer de HSEM.

6.2. Denegación de HPS

En el caso de que por la Autoridad competente no se conceda una HPS, la DGAM (SDGINSERT) comunicará dicha denegación a la empresa solicitante para su traslado a la persona interesada, que firmará un acuse de recibo, para su posterior entrega a la Autoridad que denegó la HPS.

Será motivo suficiente de denegación o retirada el que se falsee cualquiera de los datos que se requieren en el expediente de solicitud, o el que estos no se aporten en su totalidad.

La denegación, con carácter general, tendrá el efecto adicional de inhabilitar al interesado para poder solicitar nueva HPS durante los periodos siguientes:

− 3 años, para solicitar nueva HPS de grado “CONFIDENCIAL”.

− 5 años, para solicitar nueva HPS de grado “RESERVADO” y superior.

6.3. Retirada de la HPS

Se podrá proceder a la retirada de una HPS si se considera que existen motivos que lo justifican, bien de oficio, bien a petición del Jefe de Seguridad del Servicio de Protección de la empresa afectada.

En el caso de que por la Autoridad competente se retire una HPS, la DGAM (SDGINSERT), comunicará dicha retirada a la empresa, para su traslado a la persona afectada, que firmará un acuse de recibo para su posterior entrega a la Autoridad que retiró la HPS.

En caso de retirada, se aplicarán las mismas restricciones de tiempo que para la denegación de HPS.

6.4. Renovación de la HPS

La HPS se extiende, inicialmente, por un periodo de validez de cinco años. Si al terminar este período se mantiene la necesidad de seguir disponiendo de la HPS, se solicitará su renovación con antelación suficiente, para lo que se seguirán los mismos trámites y se usarán los mismos formularios que si se tratara de una solicitud inicial.

Cada renovación exige una nueva investigación de seguridad del titular de la HPS, sobre la base de la Declaración Personal de Seguridad, que deberá ser rellenado de nuevo por el interesado con datos actualizados, junto con el resto del expediente de solicitud.

La renovación se puede realizar para el mismo grado y especialidades de la que caduca, o bien, para otros diferentes, manteniendo en todos los casos el carácter de renovación.

El expediente de solicitud de renovación tendrá la misma constitución y tratamiento que una solicitud inicial, con la única salvedad de que el plazo de validez de la HPS que se conceda puede ser diferente. El periodo de validez de la HPS renovada será de cinco años en el caso de las habilitaciones de grado “SECRETO” y de diez años en el caso de las habilitaciones de grado RESERVADO y CONFIDENCIAL.

La HPS con especialidad SIGINT, se renovará siempre por cinco años, con independencia del grado de clasificación.

La HPS con especialidad CRIPTO no establece servidumbres de tiempo.

Para aquellas HPS para las que se solicite su renovación con posterioridad a la fecha de su caducidad, se considerará como una solicitud inicial, por lo que, en su caso, se le concederá por un tiempo máximo de cinco años.

Una HPS mantiene su vigencia hasta que se cumpla la fecha de caducidad de la misma. Si con antelación a la fecha de caducidad se hubiera iniciado el trámite de renovación, y estuviera en trámite de concesión, la validez de la HPS se prorrogará por un plazo máximo de seis meses, a contar desde la fecha de caducidad, con carácter automático y sin necesidad de solicitud al efecto. En estas condiciones, y sin sobrepasar el plazo indicado, se podrán emitir Certificados de HPS válidos por los órganos autorizados.

6.5. Ampliación de la HPS

La HPS se emite con un determinado grado de clasificación, que es aquél para el que se precisa, y habilita a acceder a información clasificada de dicho grado o de grado inferior.

En caso de ser necesario, se puede solicitar una ampliación de HPS, bien del grado de clasificación, como de la especialidad de Información clasificada a la que se autoriza a acceder. La ampliación se solicitará a la DGAM (SDGINSERT), concediéndose, en su caso, con la misma fecha de caducidad que la HPS original que se amplía, salvo que el nuevo grado implique un período de vigencia menor (como ocurre para grado "SECRETO", o para determinadas especialidades).

El expediente de solicitud de ampliación de HPS consta de la solicitud de Habilitación Personal de Seguridad cumplimentada de la misma forma que para una solicitud inicial.

En el caso de que se solicitara una ampliación del grado de clasificación o especialidad de la HPS, será preceptivo cumplimentar aquellos apartados de la Declaración Personal de Seguridad que no se contestaron en la anterior solicitud, y que ahora son obligatorios, en función del grado o especialidad al que se desea ampliar la nueva HPS.

No se podrá solicitar ampliación en caso de que quede menos de un año para la caducidad de la HPS a ampliar. En este caso, dados los plazos de ejecución, se solicitará directamente como una renovación.

6.6. Suspensión de la HPS

En caso de necesidad, y con motivo de una circunstancia sobrevenida o conocida que pueda afectar a la seguridad de la Información clasificada, se podrá proceder, en cualquier momento, a la suspensión de los efectos de una HPS en vigor, a la que seguirá el inicio por la Autoridad competente de un proceso de investigación del que se derivará la retirada o continuación en vigor de la HPS afectada.

Durante el periodo de suspensión, el usuario carece, a todos los efectos, de Habilitación Personal de Seguridad. La DGAM (SDG INSERT) lo comunicará al JSSP de la empresa, para que éste a su vez lo haga al usuario.

El tiempo de suspensión no tendrá efecto alguno sobre la fecha de caducidad de la HPS, no dando lugar a abonos de tiempo.

Por otra parte, el contratista solicitará a la DGAM (SDGINSERT), la suspensión de la HPS de un empleado cuando se presente alguna de las siguientes situaciones:

a) Cause baja como personal del contratista.

b) Cambie de actividad y no vaya a manejar Información clasificada.

El contratista deberá devolver, a través de la DGAM (SDG INSERT), a la Autoridad emisora el certificado de HPS correspondiente, en caso de que hubiera sido emitido.

6.7. Habilitación Personal de Seguridad Temporal

No se tramitarán solicitudes de HPS Temporal para personal de empresas o autónomos que actúen como asesores de la Administración, en el ámbito de la Seguridad Industrial.

6.8. Apelación.

Las resoluciones adoptadas en relación con las solicitudes de HPS estarán sujetas al régimen jurídico establecido en la Ley del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

6.9. HPS para personas no empleadas del contratista.

6.9.1. Personal de mantenimiento y limpieza.

Sólo en casos particulares y siempre que se trate de personal fijo, se podrá solicitar HPS para personas que presten servicios de mantenimiento o limpieza de instalaciones. En concreto, será necesario cuando dichos trabajos se realicen en una Zona de Acceso Restringido configurada como Área de Seguridad Clase I, en la que no es posible ocultar toda la Información clasificada o puede producirse con cierta probabilidad un acceso fortuito a la misma.

En estos casos, el propio Órgano de Control del que depende la Zona de Acceso Restringido, será el responsable de iniciar y tramitar el expediente de habilitación de seguridad de dicho personal. La empresa de servicios a la que pertenezca el personal no precisará disponer de una HSEM.

Al personal de mantenimiento de instalaciones y limpieza le será prohibida la entrada sin escolta en las Zonas de Acceso Restringido, aun cuando cuente con HPS. Esta escolta no necesariamente tendrá que prestarse por personal específico de seguridad, sino que podrá ser personal autorizado en dicha zona quien les acompañe. Durante su estancia en la zona, las informaciones clasificadas estarán protegidas de la observación y de la escucha pasiva o activa. Si el riesgo es mínimo, bastará con realizar una supervisión continua de la actividad de dicho personal, no quedando nunca sin control mientras permanezcan dentro de la zona.

6.9.2. Asesores del contratista

Las personas que sin tener relación laboral con el contratista sean designadas asesores externos del mismo para la preparación de una oferta o para el desarrollo de un contrato que implique acceso a materias clasificadas, deberán tener una relación contractual de prestación de servicios con el contratista y se considerarán en sus relaciones con el Ministerio de Defensa como empleados del mismo, por lo que éste deberá solicitarles la Habilitación que corresponda.

Se exceptúa el caso de aquellos asesores o consultores que, en el desempeño de sus trabajos para el contratista, vayan a manejar materias clasificadas en las dependencias propias del asesor, en cuyo caso serán considerados como subcontratistas y deberán obtener la correspondiente Habilitación de Seguridad de Empresa (HSEM), Habilitación de Seguridad de Establecimiento (HSES) y la apertura del Órgano de Control correspondiente.

Cuando los asesores o consultores que precisen acceder a materias clasificadas procedan de una Empresa de Trabajo Temporal serán considerados como empleados del contratista. El contratista solicitará de dicha empresa una memoria que incluya accionistas, relación de miembros del Consejo de Administración u órgano ejecutivo similar, relación de directivos, y relaciones con organismos y empresas extranjeras, además de un informe personal de cada asesor o consultor. Estos informes estarán a disposición del Ministerio de Defensa, al igual que los documentos que registren las necesarias relaciones contractuales.

6.9.3. Personal de Uniones Temporales de Empresas

Todo el personal de las empresas constitutivas de la UTE que precise acceder a Información clasificada deberá solicitar HPS. El personal de aquellas empresas que forman la UTE que no dispongan de HSEM podrá solicitar HPS a través del JSSP de alguna de las empresas de la UTE que sí estén en posesión de ella. En todo caso regirá al principio de que sólo se podrá acceder a Información clasificada en aquellos locales habilitados al efecto.

6.9.4. Personal en prácticas

El personal que está realizando prácticas de estudios promovido por entidades ajenas al contratista, como es el caso de los estudiantes becarios, no podrán participar en proyectos o contratos que impliquen acceso a materias clasificadas.

6.9.5. Otras personas

Las personas no empleadas directamente por el contratista, pero vinculadas contractualmente con el mismo, no incluidas en los apartados anteriores, y cuyo acceso a cualquier materia clasificada se considere necesario, deberán obtener previamente la Habilitación Personal de Seguridad del grado correspondiente, como si fuesen empleados del contratista, así como la debida Autorización de Acceso, correspondiendo al Jefe del Servicio de Protección la necesaria formación.

7. ÓRGANO DE CONTROL DE LA INFORMACIÓN CLASIFICADA

7.1. Procedimiento para apertura de un Órgano de Control por parte de un contratista.

Toda empresa que participe en programas, proyectos o contratos clasificados del Ministerio de Defensa y que no vaya a almacenar información clasificada en sus instalaciones, deberá tener concedida una HSEM y tener establecido un Servicio de Protección de materias clasificadas (SPMC) y un Órgano de Control.

El Órgano de Control puede ser:

- Servicio Local de Protección de materias clasificadas (SLPMC) para manejo de Información clasificada. Cuando así lo aconseje la distribución geográfica de la empresa o la gran extensión de una instalación de la misma, el contratista podrá solicitar la constitución de varios SLPMC. Además, el contratista podrá disponer de varias ZAR, dependientes del mismo Órgano de Control.

- Servicio General de Protección de materias clasificadas (SGPMC), en caso de tener varios SLPMC.

- Cuenta cripto. Para manejo de material de cifra (documentación, claves, y equipos).

En el caso de que la empresa vaya a almacenar o manejar Información clasificada en sus instalaciones, deberá tener concedida, además de la HSEM, del Servicio de Protección de materias clasificadas y del Órgano de control de materias clasificadas que corresponda, una HSES,

Cada Órgano de Control está formado por el conjunto de personal, recursos materiales y procedimientos que, actuando coordinadamente, tienen como finalidad proteger la Información clasificada de los riesgos que pudiera provocar el acceso no autorizado a la misma, o afectar a su integridad y disponibilidad.

El cargo de Jefe de Seguridad del Servicio Local/General de Protección (SLPMC/SGPMC) es compatible con el de Jefe de Seguridad del Servicio de Protección (JSSP).

<u>Composición del Órgano de Control</u>

El Órgano de Control está integrado por el Jefe de Seguridad (JSSLP o JSSGP), su suplente (JSSLP suplente o JSSGP suplente), así como, en su caso, por el Administrador de Seguridad de los Sistemas de Información y Comunicaciones (ASSI), si lo hubiera.

Por su parte, la apertura de una Cuenta Cripto requerirá el nombramiento de un Criptocustodio, como responsable de la misma, y de un Criptocustodio alterno, que asumirá todas las responsabilidades y obligaciones de aquel en su ausencia.

Los componentes del Órgano de Control deberán tener HPS conforme al grado de la HSES, y tener nacionalidad española.

Para solicitar la apertura de un Órgano de Control, el procedimiento a seguir dependerá de si se va a almacenar o no Información clasificada en las instalaciones de la empresa.

Primer caso: La empresa sí va a almacenar información clasificada en sus instalaciones.

La empresa dirigirá por escrito solicitud de apertura del Servicio General o Local de Protección (SGPMC o SLPMC), y/o cuenta cripto a la DGAM (SDGINSERT). A este escrito unirá como anexo el Plan de Protección de la/s ZAR que se pretenda acreditar, y la Propuesta de Personal de los responsables del Órgano de Control, recogida en el formulario de solicitud de HPS existente en el anexo II.

El Plan de Protección será confeccionado siguiendo las directrices que se indican a continuación. El Plan de Protección consta de tres documentos diferenciados:

− El Plan de Acondicionamiento.

− El Plan de Seguridad.

− El Plan de Emergencia.

A modo orientativo, para la elaboración del Plan de Protección y la constitución de la Zona de Acceso Restringido, se puede consultar, respectivamente, en:

Orientaciones para el Plan de Protección:

http://www.cni.es/comun/recursos/descargas/OR-ASIP-01-01_03_Orientaciones_para_el_Plan_de_Proteccion_de_una_ZAR.pdf

Orientaciones para la constitución de ZAR:

http://www.cni.es/comun/recursos/descargas/OR-ASIP-01-02_03_Orientaciones_para_la_Constitucion_de_ZAR.pdf

Es recomendable su confección en formato electrónico, para facilitar su posterior actualización. En este sentido, es fundamental que refleje, en todo momento, la situación real de la seguridad de la empresa, por lo que habrá que actualizarlo cada vez que haya cambios en la misma.

Los componentes del Órgano de Control recibirán la instrucción necesaria para llevar a cabo sus misiones. El nombramiento de los componentes del Órgano de Control está supeditado a la asistencia y superación de los cursos de instrucción que se determine.

Si es correcta la documentación entregada, se comunicará por escrito a la empresa, la apertura del Órgano de Control, indicándole que tiene capacidad para almacenar información clasificada en sus instalaciones hasta el grado que corresponda, así como la dependencia funcional que adquiere.

Segundo caso: La empresa no va a almacenar Información clasificada en sus instalaciones.

La empresa, que debe contar con HSEM, sólo tiene que solicitar la apertura del Órgano de Control (SLPMC/SGPMC/cuenta cripto) por escrito a la DGAM (SDGINSERT), adjuntando al mismo las Propuestas de Personal de sus responsables, previa cumplimentación del correspondiente formulario PP-103 del anexo II.

Si es correcta la documentación entregada, se comunicará por escrito a la empresa la apertura del Órgano de Control, indicándole que no tiene capacidad para almacenar Información clasificada en sus instalaciones, así como la dependencia funcional que adquiere.

7.2. Procedimiento para el cierre de un Órgano de Control por parte de un contratista

Para proceder al cierre de un Órgano de Control de una empresa, ésta deberá solicitarlo por escrito, firmado por el responsable de la empresa o su apoderado, a la DGAM (SDGINSERT), de la que depende funcionalmente, a la que le hará entrega, antes de producirse el cierre efectivo, de toda la Información clasificada que tuviera bajo su custodia, así como los libros de registro, actas de destrucción y resto de documentación relevante que obre en su poder.

8. PROCEDIMIENTO PARA EL TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA

8.1. Acceso a la Información clasificada

Se podrá acceder a materias clasificadas, de grado "CONFIDENCIAL" o superior, cuando se cumplan los siguientes requisitos:

1. Tener necesidad de conocer por razón de la función que se desempeñe.
2. Tener vigente la Habilitación Personal de Seguridad expedida por la Autoridad competente de igual o superior grado que el asignado a la materia clasificada.
3. Haber recibido la instrucción de seguridad preceptiva.
4. Estar informado, reconocido expresamente, de las responsabilidades y compromisos que implica dicho acceso.
5. Tener Autorización de Acceso expresa a la materia clasificada de que se trate. Para obtener dicha autorización, habrá de emplearse el formulario del anexo VIII.

Las personas que solo necesiten acceder a información clasificada del MINISDEF con un grado de clasificación de DIFUSIÓN LIMITADA, deberán haber sido instruidas en sus responsabilidades de seguridad y habrán de tener "necesidad de conocer". No se necesitará habilitación personal de seguridad para acceder a información clasificada de este grado.

Deberán disponer de HPS no solo las personas que manejan la información clasificada de grado "CONFIDENCIAL o superior, sino también los encargados de su custodia y traslado y, en general, cualquiera que pudiera tener la posibilidad razonable de acceso a la misma.

Toda persona que está accediendo a materias clasificadas, deberá poder identificarse en cualquier momento.

8.2. Grados de clasificación de seguridad

El MINISDEF como originador de la información es el responsable de la aplicación de los criterios de clasificación definidos en una directiva/guía de clasificación, y por tanto, proponer la clasificación de seguridad de la información y su difusión inicial.

Una vez aprobado por la Autoridad correspondiente, el grado de clasificación de la información, no podrá cambiarse, reducirse ni eliminarse sin el consentimiento del MINISDEF. En el momento de su creación, el MINISDEF como originador indicará, siempre que sea posible, si el grado de clasificación de la información puede reducirse o eliminarse en cierta fecha o casos. Es prerrogativa del MINISDEF como propietario de la información proponer a la Autoridad correspondiente la modificación de la clasificación de seguridad durante su ciclo de vida.

Los grados de clasificación nacional en España, de mayor a menor, son los siguientes:

- SECRETO (S)
- RESERVADO (R)

- CONFIDENCIAL (C)
- DIFUSIÓN LIMITADA (DL)

8.3. Requisitos de imputabilidad.

La información clasificada de grado “RESERVADO” o superior es información imputable, por lo que, además del control llevado a cabo por el sistema de registro, de forma adicional debe ser registrado todo acceso que se produzca a dicha información, con indicación inequívoca de la persona que accede, fecha-hora en que se produce el acceso y registro de firma

8.4. Capacidad para clasificar.

En el ámbito Nacional, la facultad para clasificar de SECRETO y RESERVADO corresponde al Consejo de Ministros y a la Junta de Jefes de estado Mayor, no pudiendo ser transferida ni delegada. La Ley de Secretos Oficiales no contempla grados de clasificación inferiores, por lo que éstos se definen y rigen por normativa de desarrollo de dicha Ley.

Tendrán facultad para clasificar de CONFIDENCIAL o DIFUSIÓN LIMITADA en el ámbito del MINISDEF, las siguientes autoridades, pudiendo delegar oficialmente dicha atribución: El Ministro, el Jefe del Estado Mayor de la Defensa, el Secretario de Estado de Defensa, el Subsecretario de Defensa, el Secretario General de Política de Defensa, el Jefe del Estado Mayor del Ejército, el Jefe del Estado Mayor de la Armada y el Jefe del Estado Mayor del Ejército del Aire.

8.5. Distribución de la Información clasificada.

La distribución e intercambio de información clasificada se realizará entre Órganos de Control de un mismo contratista, con las particularidades que se exponen a continuación para cada grado de clasificación.

La Información clasificada de grado “SECRETO” circulará siempre a través de los Servicios Generales y Centrales de Protección de información clasificada del MINISDEF, no pudiendo almacenarse nunca en los Órganos de Control de los contratistas

La Información clasificada de grado “RESERVADO” circulará siempre a través del correspondiente Servicio General de Protección de Materias Clasificadas del MINISDEF, informando al Representante para la Seguridad del Contrato o Programa afectado.

La Información clasificada de grado “CONFIDENCIAL”, podrá circular directamente entre los Órganos de Control de un mismo contratista, siendo preciso informar al Representante para la Seguridad del Contrato o Programa afectado, de los movimientos producidos. Cuando la circulación haya de producirse entre diferentes contratistas, se realizará a través del correspondiente Servicio General de Protección de Materias Clasificadas del MINISDEF.

La información clasificada de grado “DIFUSIÓN LIMITADA” podrá intercambiarse directamente entre Órganos de Control de un mismo contratista.

En el caso de que Información clasificada tenga un destinatario concreto, el Órgano de Control al que llegue la información se lo comunicará al interesado, quien los examinará en las instalaciones autorizadas, no pudiendo extraer la información del Órgano de Control.

Toda materia clasificada que sea transferida deberá ir acompañada del correspondiente Recibo de Materias Clasificadas (Ver anexo IX) cumplimentado en todos sus apartados.

Los recibos se archivarán mientras sea necesario justificar la situación de las materias clasificadas, así como para demostrar, en su caso, la devolución o entrega de las mismas.

Cuando se reciba cualquier materia clasificada, se seguirá el siguiente proceso:

1. Se examinarán los envíos para asegurarse de que no han sido violados, comprobándose el contenido con el recibo. La evidencia de violación y las anomalías que se observen en el contenido deberán notificarse inmediatamente al remitente y a la DGAM (SDGINSERT).
2. Cuando el envío esté en orden, se firmará el recibo y se devolverá debidamente cumplimentado al remitente. Inmediatamente, el Jefe del Servicio de Protección hará la oportuna anotación en el Libro Registro.

8.6. Reproducción, traducción, y extractos de la Información clasificada.

En el ámbito empresarial, los usuarios podrán realizar copias, extractos y traducciones de Información clasificada de grado “DIFUSIÓN LIMITADA” siempre que se garantice que las mismas van a ser usadas por personal del mismo contratista de quien las realizó, se cumpla el principio de necesidad de conocer, hayan sido instruidos en el manejo de Información clasificada y se disponga de la autorización de acceso correspondiente.

En el ámbito empresarial, los Jefes de Seguridad de los Órganos de Control podrán realizar, para su propio personal, copias, extractos y traducciones de Información clasificada de grado “CONFIDENCIAL” cuando sea necesario por motivos de trabajo, asegurándose que a cada copia, extracto o traducción se le asigna un número de documento y que éstos quedan convenientemente registrados, siendo preceptiva la autorización del correspondiente SPMC del MINISDEF y la comunicación al Representante para la Seguridad del Contrato o Programa afectado, y, en su caso, al Inspector de Seguridad que tuviera nombrado la empresa.

Las reproducciones tendrán la misma clasificación que el original y su estampillado será controlado por el Inspector de Seguridad.

Los Jefes de Seguridad de los Órganos de Control de los contratistas, previa autorización del correspondiente SPMC del MINISDEF, podrán realizar, para su propio personal, copias, extractos o traducciones de Información clasificada de grado “RESERVADO”, cuando sea necesario por motivos de trabajo, asegurándose que a cada copia, extracto o traducción tiene asignado el número de registro que corresponda, adicional al de referencia,

En el ámbito empresarial, queda expresamente prohibida la realización de copias de Información clasificada de grado “SECRETO”.

La autorización para reproducir o transmitir materias clasificadas se plasmará en el documento correspondiente, según anexo X.

8.7. Destrucción de la Información clasificada

El Ministerio de Defensa podrá autorizar al contratista a destruir materias clasificadas cuando sea oportuno, debiéndose cumplimentar el Acta de destrucción de materias clasificadas contemplada en el anexo XI. No obstante se tendrá en cuenta lo establecido en la Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos (SEGINFODOC) en lo relativo a la destrucción de documentos originales.

La Información clasificada de grado "DIFUSIÓN LIMITADA" podrá ser destruida directamente por los Jefes de Seguridad de los Órganos de Control de los contratistas sin que se precise su comunicación a su órgano superior.

La destrucción de Información clasificada de grado "CONFIDENCIAL" la ~~se~~ realizará el Jefe del Servicio Local/General de Protección de Materias Clasificadas~~-~~ del contratista, previamente autorizado por el correspondiente SPMC del Ministerio de Defensa, ante la presencia del Inspector de Seguridad, en caso de que esté nombrado, debiéndose cumplimentar el acta de destrucción de materias clasificadas del anexo XI, que deberá remitirse al Representante para la Seguridad del Contrato o Programa afectado. La destrucción se anotará en el Libro de Registro.

La Información clasificada de grado "RESERVADO" sólo podrá ser destruida, ante la presencia del Inspector de Seguridad, en caso de que esté nombrado, en aquellos Órganos de Control de los contratistas que hayan sido autorizados para ello por el correspondiente SPMC del Ministerio de Defensa, debiéndose cumplimentar el acta de destrucción de materias clasificadas del anexo XI que será firmada por el responsable del Órgano de Control que realice su destrucción y por una persona, preferiblemente ajena al Órgano de Control, que actuará como testigo del acto y que deberá disponer de la HPS correspondiente, al menos al grado de clasificación del documento que se va a destruir.

Una vez cumplimentada el acta, se deberá remitir al correspondiente SPMC del MINISDEF e informando al Representante para la Seguridad del Contrato o Programa afectado. La destrucción se anotará en el Libro de Registro.

Queda expresamente prohibida a los contratistas la destrucción de Información clasificada de grado "SECRETO.

La destrucción se hará de forma tal que se garantice que las materias clasificadas queden irreconocibles y se impida su reconstrucción total o parcial. El contratista se asegurará de la eficacia del proceso de destrucción utilizado.

Se deberá destruir regularmente, cumplimentando la citada acta, todo material de trabajo como borradores, cintas de máquina, soportes informáticos removibles etc. que se hayan utilizado en el tratamiento de información clasificada, y por tanto, puedan incluir restos de dicha información a pesar de haber efectuado un borrado.

8.8. Registro de materias clasificadas

En los Órganos de Control del contratista, existirá un Libro Registro o sistema alternativo donde figurará anotada toda materia clasificada que haya tenido entrada o salida, así como las reproducciones, destrucciones y el acceso a dichas materias clasificadas por personal tanto propio como ajeno al contratista.

El Libro Registro, dado su contenido, no deberá recoger anotaciones clasificadas de ningún tipo, sino solamente referencias a las mismas. Estará permanentemente sujeto a su inspección y tendrá que ser cumplimentado y convenientemente custodiado por el Jefe de Seguridad del Servicio de Protección del contratista (JSSP). El empleado que lo utilice circunstancialmente en sustitución del JSSP, deberá tener Habilitación Personal de Seguridad.

8.9. Devolución de materias clasificadas

La devolución de materias clasificadas por el contratista al Ministerio de Defensa deberá realizarse ajustándose a las siguientes instrucciones:

1 .Cuando una oferta no haya sido presentada dentro del plazo establecido, deberán devolverse las materias clasificadas recibidas para la elaboración de dicha oferta, dentro de los quince (15) días naturales siguientes a la expiración del plazo de presentación.

2. Cuando una oferta no haya sido adjudicada, la devolución se hará dentro de los treinta (30) días naturales a partir de la notificación.

3. Cuando una oferta resulte adjudicada, la devolución se hará dentro de los tres meses siguientes a la finalización de los trabajos, si no dispone lo contrario el Ministerio de Defensa.

En caso de retirada de la Habilitación de Seguridad de Empresa, el Ministerio de Defensa fijará el plazo de devolución de todas las materias clasificadas que obren en poder del contratista.

El contratista deberá devolver al correspondiente SGPMC de empresas del Ministerio de Defensa todas las materias clasificadas que le hayan sido facilitadas, incluidas todas las reproducciones. Asimismo entregará toda aquella desarrollada por el propio contratista en relación con dicho contrato, que incluya Información clasificada.

El contratista no podrá utilizar las materias clasificadas para otros contratos sin la expresa autorización del Ministerio de Defensa. La solicitud para que un contratista mantenga en depósito materias clasificadas fuera de los plazos señalados, deberá hacerse por escrito, e irá dirigida al Jefe del Órgano Responsable del Contrato.

El incumplimiento de los plazos de devolución de materias clasificadas al Ministerio de Defensa podrá determinar, en su caso, la retirada de la Habilitación de Seguridad de Empresa, al margen de otras responsabilidades que se pudieran derivar.

8.10. Inventario anual

El contratista presentará ante el Órgano de Contratación, Servicio Proponente u Oficina de Programa del Ministerio de Defensa responsable del Contrato, antes del 31 de diciembre de cada año, un inventario anual de todas las materias clasificadas que obren en su poder referente a cada contrato.

9. PROCEDIMIENTO PARA EL TRATAMIENTO DE LA INFORMACIÓN ORIGINADA POR EL CONTRATISTA SUSCEPTIBLE DE SER CLASIFICADA

Cuando un contratista origine, como consecuencia de una oferta o contrato del Ministerio de Defensa, información que deba señalarse como clasificada, realizará la solicitud al Órgano de Contratación, a través del Representante para la Seguridad del Contrato o Programa, e informará de ello al Inspector de Seguridad, debiendo protegerla como tal Información clasificada, responsabilizándose en caso de omisión.

Para el marcado de documentos se seguirá lo dispuesto en la SEGINFODOC.

Si el contratista observa una posible falta o defecto en la clasificación, lo pondrá en conocimiento del correspondiente SPMC del Ministerio de Defensa, adoptando provisionalmente la protección que considere adecuada, siempre que sea de grado superior, hasta recibir las instrucciones pertinentes.

Si el contratista estableciera algún procedimiento para identificar documentación propia, deberá utilizar marcas y estampillas claramente diferenciables de las establecidas reglamentariamente para las materias legalmente clasificadas.

10. PROCEDIMIENTO SOBRE VISITAS CON ACCESO A INFORMACIÓN CLASIFICADA

A efectos de estos procedimientos, se consideran visitas aquellas personas que, sin tener una relación de dependencia directa con el contratista, acceden física y circunstancialmente, por temas profesionales, a las dependencias o a los empleados del mismo.

Las visitas se inscribirán en el Libro de Registro de Visitas o sistema alternativo del contratista, que deberá recoger: Fechas de la visita, nombre completo del visitante, número del DNI o del pasaporte, nacionalidad, empresa/organismo o dirección del visitante, y nombre de la persona visitada. Este registro estará a disposición del Ministerio de Defensa, siempre que sea requerido.

10.1. Visitas de extranjeros

El contratista visitado será responsable del control del acceso a las materias clasificadas, que ha de limitarse a aquélla para la que el Ministerio de Defensa conceda la debida Autorización de Acceso. En todo caso, el número de visitas de extranjeros con acceso a materias clasificadas será el mínimo imprescindible, debiendo cumplirse los siguientes requisitos:

1. Que las autorizaciones de acceso sean solicitadas por el contratista visitado, cumplimentando el formulario del anexo VIII, que deberá ir acompañado por una certificación oficial (Request For Visit – RFV, anexo XIV) de que el visitante extranjero posee Habilitación Personal de Seguridad o equivalente en su país.

2. Que la solicitud de la autorización de acceso tenga registrada su entrada en la Dirección General de Armamento y Material (SDGINSERT) con una antelación mínima de veinte (20) días naturales al inicio de la visita.

3. El acceso a la Zona Clasificada o a las materias clasificadas se anotará en el Libro Registro de Visitas, o sistema alternativo, del contratista.

4 Una vez concluida la visita, el Jefe de Seguridad del Servicio de Protección remitirá, en un plazo no superior a cinco (5) días, a contar desde que la visita finalice, el formulario Informe de Visitas recogido en el anexo XV al Ministerio de Defensa, debida y completamente formalizado.

10.2. Personal del Ministerio de Defensa

El personal del Ministerio de Defensa, para poder tener acceso a materias clasificadas en poder de un contratista, deberá tener la correspondiente Autorización de Acceso del Órgano del Ministerio de Defensa Responsable del Contrato, quien comunicará la resolución de la visita al contratista. De este trámite quedan exentos los Inspectores de Seguridad en el cumplimiento de su misión como tales.

10.3. Visitas de Españoles no pertenecientes al Ministerio de Defensa

Se seguirán los siguientes procedimientos:

1. Las Autorizaciones de Acceso, recogidas en el anexo VIII, serán solicitadas por el contratista visitado.

2. La solicitud de la Autorización de Acceso tendrá su entrada en la Dirección General de Armamento y Material (SDGINSERT) con una antelación mínima de cinco (5) días al inicio de la visita.

3. El acceso a la Zona Clasificada o a las materias clasificadas se anotará en el Libro Registro de Visitas o sistema alternativo del contratista.

10.4. Información de responsabilidad

Antes de producirse el acceso a materia clasificada, los visitantes deberán ser advertidos por el Jefe de Seguridad del Servicio de Protección, o persona designada por éste, sobre la responsabilidad que contraen accediendo a materias clasificadas, protegidas por la legislación española y por los tratados internacionales que amparan dicho acceso; y por tanto del compromiso legal de no difundir su conocimiento a personas no autorizadas expresamente.

10.5. Control de visitas

Los visitantes autorizados deberán realizar su identificación antes de iniciar la visita. El contratista no permitirá el acceso a la Zona Clasificada y a la materia clasificada, hasta que esté seguro de la identidad y haya verificado que los datos aportados coincidan con los que constan en la debida Autorización de Acceso.

Para el control de las visitas se seguirán las siguientes normas:

1 .El contratista controlará el movimiento de las visitas que entren en sus dependencias, para garantizar la debida seguridad de las materias clasificadas que custodie.

2. Se prohibirá al visitante efectuar cualquier tipo de registro o reproducción de las materias clasificadas, si no existe una autorización previa por escrito del Ministerio de Defensa.

3. No podrá entregarse al visitante material o documentación clasificada para llevar fuera de las ZAR y dependencias del contratista, sin la debida autorización previa por escrito del Ministerio de Defensa.

10.6. Visitas recurrentes o de larga duración

Tendrán esta consideración las realizadas de forma repetitiva durante un período de doce (12) meses, por lo que se solicitarán una sola vez.

Si el contratista considera que, una vez finalizado el periodo de doce (12) meses, la visita debe continuar o se va a reiterar, solicitará la autorización nuevamente.

En ningún caso la visita de larga duración podrá encubrir una relación laboral entre el contratista visitado y el visitante.

Cuando se interrumpan definitivamente las visitas de larga duración, el contratista deberá notificarlo inmediatamente al Ministerio de Defensa, para que se proceda a cancelar su autorización, remitiendo el correspondiente Informe de Visitas recogido en el anexo XV al Ministerio de Defensa, debida y completamente formalizado.

10.7. Visitas relacionadas con programas multinacionales o en el ámbito de acuerdos internacionales

En el marco de un programa multinacional o en el ámbito de un acuerdo internacional pueden producirse visitas de extranjeros a España o de españoles al extranjero con acceso a materias clasificadas.

En ambos casos, estas visitas se regirán por las normas aprobadas específicamente para dicho programa o acuerdo.

La Autorización de Acceso la otorgará la Autoridad que corresponda según las normas específicas del programa o acuerdo.

Esta Autorización podrá concederse en base a la acreditación de estar en posesión de la debida habilitación de seguridad, que será realizada por la Autoridad nacional con responsabilidad en la protección de la información clasificada del país de procedencia del visitante.

La acreditación se podrá obtener tramitando el formulario RFV, anexo XIV, conforme a las normas específicas del programa o acuerdo, o en su defecto, a través del Ministerio de Defensa (Dirección General de Armamento y Material, SDGINSERT), en los plazos que se acuerden.

10.8. Visitas tramitadas por el procedimiento de urgencia

Cuando no sea posible respetar los plazos establecidos en el procedimiento ordinario para la tramitación de una visita, relacionada con un Programa o Contrato clasificado y la no realización de la misma tenga unas consecuencias graves para el desarrollo del mismo o suponga la pérdida de una oportunidad de negocio, ésta será considerada como “Visita Urgente”, lo que significa que se podrá tramitar al margen de dichos plazos.

Las visitas de emergencia serán aprobadas como visitas por una sola vez.

Toda visita que se derive de una visita de emergencia deberá ser tramitada por el procedimiento ordinario.

Las visitas de emergencia deberán ir acompañadas de la correspondiente justificación, que será evaluada por la Autoridad competente.

11. PROCEDIMIENTO PARA REALIZACIÓN DE TRANSPORTES CLASIFICADOS EN EL ÁMBITO INDUSTRIAL.

El envío por cualquier medio, sea físico o tecnológico, de Información clasificada de un remitente a un destinatario, bien personas o bien Órganos de Control, constituye una transmisión de Información clasificada.

Esta transmisión se puede hacer por medios físicos, como pueden ser el correo postal, transporte personal, correo oficial diplomático o militar, etc., que es lo que se conoce habitualmente como transporte, y también puede realizarse por medios tecnológicos, por ejemplo transmisión por fax, teléfono u otras tecnologías de la información y de las comunicaciones (TIC) debidamente acreditadas.

Como norma general, el método preferible de transmisión de Información clasificada, no sólo por cuestiones de inmediatez, sino también por la mayor seguridad y menor riesgo que supone, será el de transmisión por medios tecnológicos. En segunda preferencia estará el transporte en soportes informáticos protegidos por un producto criptológico aprobado. En este caso tendrá el mismo tratamiento y se podrá transportar por los mismos medios que si se tratara de información no clasificada, por lo que no precisará medidas especiales de protección de la confidencialidad.

No obstante, cuando se transporte en mano, el portador llevará las autorizaciones necesarias que le identifiquen como persona autorizada, aunque no precise de Habilitación Personal de Seguridad (HPS).

En adelante, al establecer criterios para el transporte, se hará sobre la base de que la Información clasificada que se transmite está en claro, por ser el caso más desfavorable.

Solamente está previsto el procedimiento para transportar Información clasificada de grado RESERVADO, CONFIDENCIAL o DIFUSIÓN LIMITADA, pero no de grado SECRETO, no pudiendo transportar este tipo de información por ningún medio, dado que nunca estará en poder de las empresas contratistas.

11.1. Transporte de Información clasificada de grado CONFIDENCIAL o RESERVADO

11.1.1. Transporte Personal de Información clasificada

Solo se podrá transmitir Información clasificada entre los contratistas de un contrato o programa clasificado por este medio en caso de necesidad urgente.

El personal designado como Correo deberá ser empleado del contratista remitente o del destinatario, o de un organismo participante en el programa o contrato clasificado que motive el transporte.

El Correo debe estar en posesión de HPS adecuada al máximo grado de la Información clasificada transportada.

El Correo deberá llevar consigo durante todo el trayecto el documento “Certificado de Correo”, recogido en el anexo XVI.

Es responsabilidad del JSSP remitente asegurarse de que el Correo y escoltas autorizados (si los hubiere) tienen toda la documentación necesaria para efectuar el

transporte (pasaporte, visado, seguro médico, moneda, licencias de exportación, etc.).

Antes de emitir el Certificado de Correo el JSSP remitente debe:

a) Informar al Correo sobre cualquier riesgo concerniente al transporte concreto.

b) Instruir al Correo en lo referente a la normativa de seguridad aplicable y responsabilidades que asume.

Una vez recibidas las instrucciones y la formación, el Correo firmará al JSSP remitente la Declaración de Instrucción, en la que manifiesta haber recibido y comprendido las instrucciones y que conoce y se compromete con las obligaciones contraídas.

Una vez realizado el transporte, el Correo firmará al JSSP destinatario o persona debidamente autorizada el apartado 5 “Finalización de la misión” del anexo XVI y entregará ese documento, como Recibo de Entrega. En el caso de que se haya producido algún incidente durante el recorrido, se informará a los JSSP remitente y destinatario, que a su vez informarán a la DGAM (SDGINSERT).

11.1.2. Transporte de Información clasificada como mercancía

Cuando la Información clasificada a transportar sea de un tamaño, peso o cualquier otra característica que aconseje su transporte como mercancía, los JSSP remitente y destinatario deberán elaborar conjuntamente un plan de transporte, que será remitido para su supervisión o autorización, en el caso de transporte nacional, por la SDGINSERT de la DGAM con una antelación mínima de:

a) Siete (7) días naturales al inicio previsto del transporte cuando se trate de un transporte nacional.

b) Diez (10) días naturales al inicio previsto del transporte cuando se trate de un transporte internacional.

Al mismo tiempo, el JSSP remitente deberá preparar dos copias de un Recibo de Transporte de Material Clasificado, según el modelo recogido en el anexo XVII.

Una vez firmado por el JSSP destinatario, la primera copia será devuelta al JSSP remitente tras la finalización del transporte y la segunda será entregada al JSSP destinatario.

Embalaje de documentación clasificada

Se llevará a cabo de la siguiente forma:

1. La cubierta interior estará cerrada de forma que se pueda detectar su apertura, y será debidamente estampillada con el distintivo del grado de clasificación correspondiente al más alto de la información que contenga. El estampillado estará controlado por el Inspector de Seguridad, en el caso de que estuviera nombrado. Esta cubierta contendrá las direcciones del remitente y del destinatario, con identificación exacta de las personas que se responsabilizan tanto de la recepción como del envío.
2. La cubierta exterior estará cerrada y lacrada, y sólo figurarán las direcciones del receptor y del remitente, sin que conste ninguna referencia a la información que contiene.

3. Adjunto a la cubierta interior, y protegido por la cubierta exterior, se remitirá el correspondiente Recibo de Materias Clasificadas, (anexo IX). El duplicado del recibo deberá considerarse pendiente mientras no llegue al remitente el recibo firmado por el receptor. Si no lo recibiera en un período razonable, se investigarán las causas y, si se apreciasen anomalías, se dará cuenta al Inspector de Seguridad.

4. Las cubiertas, tanto interior como exterior, serán opacas y de tal naturaleza y resistencia que deberán asegurar su integridad durante el transporte, sin que se pueda desvelar su contenido.

11.1.3. Plan de Transporte

Se elaborará por el Jefe del Servicio de Protección y estará sometido a la revisión o autorización, en el caso de transporte nacional, por la DGAM (SDG INSERT). El Plan de Transporte contemplará los siguientes puntos:

1. Fecha de inicio y final del mismo, con indicación del horario previsto.

2. Direcciones exactas de salida y llegada, y descripción de los itinerarios previstos y alternativos.

3. Identificación completa del transportista comercial, en su caso.

4. Medio de transporte y datos identificativos. En caso de transporte por carretera, identificación completa de los conductores.

5. Descripción del embalaje que contiene la materia clasificada.

6. Paradas y lugares de pernocta.

7. Pasos fronterizos o aduanas.

8. Identificación de los Correos Autorizados, grado de la Garantía Personal de Seguridad que disponen, empresa a la que pertenece y descripción de la dotación y medios disponibles.

9. En caso de tener que constituirse una Zona de Acceso Restringido Especial, se especificará lugar, fecha, y tiempo de duración, con descripción detallada de dicha zona y del dispositivo de seguridad previsto.

10. Identificación completa y exacta tanto del emisor como del receptor de la materia clasificada.

11. Medios y procedimientos de enlace con los contratistas emisor y receptor.

11.1.4. Empresas de transporte de Información clasificada

Para el transporte de Información clasificada, el contratista encargado de la realización del mismo deberá:

a) Disponer de HSEM y de personal debidamente habilitado.

b) Proteger permanentemente el cargamento o vehículo mientras contenga Información clasificada. Este servicio podrá ser prestado por personal del contratista o por personal de una empresa de seguridad privada. Regirá para este personal la necesidad de tener HPS para el máximo grado de información a proteger durante el transporte, y deberá disponer del correspondiente Certificado de Correo.

c) Establecer las ZAR que le sean requeridas para el almacenamiento temporal de la Información clasificada objeto del transporte.

Salvo que deba almacenar la Información clasificada en sus instalaciones, no será necesario que disponga de HSES.

Cuando el transporte se realice en territorio nacional y el contratista remitente disponga de personal que actúe como Correo autorizado de la carga durante el recorrido, podrá hacer uso de una empresa de transporte comercial sin HSEM, para lo cual deberá asegurarse de que el personal del transportista no tenga acceso a la Información clasificada objeto del transporte.

El transportista se comprometerá por escrito ante el contratista remitente a:

a) Cumplir el plan de transporte.

b) Proporcionar un vehículo de transporte con las medidas de seguridad correspondientes a la carga.

c) Poner en conocimiento del contratista remitente los datos identificativos del vehículo utilizado y de sus conductores.

d) Observar durante el transporte las indicaciones del Correo autorizado.

11.2. Transporte de Información clasificada de grado DIFUSIÓN LIMITADA

Los JSSP remitente y destinatario deberán acordar los detalles del transporte y serán responsables de la correcta remisión y recepción del mismo para lo que deberán acordar con detalle el medio de transmisión.

La Información clasificada será transmitida de tal forma que esté sometida a continua contabilidad y trazabilidad. Es necesario que la transmisión y custodia de esta Información clasificada sea controlada por un sistema de recibos.

La Información clasificada de grado DIFUSIÓN LIMITADA podrá ser transmitida haciendo uso de transportistas comerciales que no estén en posesión de HSEM, ni que su personal posea HPS. No obstante, la empresa transportista comercial deberá cumplir los siguientes criterios:

a) Deberá estar domiciliada en España y tener implementada una política de seguridad para el manejo de material valioso. Esta política debe incluir un sistema de recibo, monitorización, control y contabilidad de la mercancía a lo largo del recorrido.

b) Debe aportar al remitente un recibo de recepción firmado de la mercancía.

c) La entrega debe producirse en el plazo de tiempo requerido.

d) Podrá subcontratar siempre y cuando exista el compromiso de respetar los criterios arriba establecidos. La responsabilidad en todo caso permanecerá en la empresa de transporte comercial contratista principal.

12. INSPECCIONES DE SEGURIDAD PARA EL SEGUIMIENTO DE CONTRATOS CLASIFICADOS

Constituyen el medio por el que el Ministerio de Defensa comprueba el cumplimiento, por parte del contratista, de las obligaciones que le corresponden en relación con su participación en contratos, programas y proyectos clasificados del Ministerio de Defensa en los que está involucrado.

Con objeto de garantizar al máximo posible la protección de la Información clasificada que el Ministerio de Defensa ponga a disposición de las empresas que participen en contratos o programas promovidos por el mismo, el Director General de Armamento y Material (DIGAM) podrá nombrar **Inspectores de Seguridad,** los cuales cesarán en el cargo a la finalización del contrato o programa.

El DIGAM notificará al contratista la identidad del Inspector de Seguridad que le haya sido asignado para la ejecución de un determinado contrato, así como, en su caso, los cambios de Inspector que se puedan producir.

El contratista se compromete a reconocer las competencias de dicho Inspector y a facilitarle su labor, disponiendo los medios necesarios para que realice sus funciones con eficacia.

En caso de tener que simultanear las labores de inspección con otras diferentes que le sean asignadas, lo hará sin menoscabo de las misiones de inspección de seguridad, que tienen carácter prioritario.

12.1. Misiones del Inspector de Seguridad

- Representará al Ministerio de Defensa ante la empresa, durante la ejecución de un contrato clasificado, en los aspectos relativos a la seguridad de la información del Departamento.

- Controlará el marcado de la Información clasificada que genere o reproduzca la empresa, previa autorización del Órgano responsable del contrato o programa.

- Velará por el cumplimiento, en el ámbito industrial y tecnológico, de lo establecido en las correspondientes Instrucciones de Seguridad de los Programas y Cláusulas de Seguridad de los contratos e informará de cualquier circunstancia que estime pueda afectar a la seguridad de la información y, en particular, de las modificaciones acaecidas en el Servicio de Protección de la empresa.

- Certificará la necesidad que tienen los empleados de la empresa de solicitar Habilitación Personal de Seguridad (HPS), en base a la función que desempeñen o puedan desempeñar en un determinado contrato o programa, firmando en su caso la solicitud de Habilitación Personal de Seguridad.

12.2. Labores de Inspección de seguridad

Constituyen el medio por el que el Inspector de Seguridad lleva a cabo las misiones recogidas en el apartado anterior.

Si como consecuencia de la realización de estas labores de inspección, el Inspector de Seguridad observara algún incumplimiento, durante la ejecución del contrato, relativo

a la seguridad de la información, remitirá informe a la DGAM (SDGINSERT), dando, asimismo, conocimiento al contratista de las irregularidades observadas, e indicándole el plazo para la corrección de las mismas.

Transcurrido dicho plazo sin que el contratista haya corregido dichas irregularidades, la DGAM (SDGINSERT), una vez hechas las comprobaciones que estime oportunas, dará conocimiento de ello al Órgano de Contratación.

13. PROCEDIMIENTO PARA LA ACREDITACIÓN DE LOS SISTEMAS CIS.

Para el manejo y custodia de Información clasificada en un Sistema de Información y Comunicaciones, el contratista deberá tener concedida en primer lugar una HSEM y una HSES del grado correspondiente a la información a tratar en los sistemas y deberá solicitar, además, la Acreditación del Sistema de Información y Comunicaciones y el nombramiento de un Administrador de Seguridad de los Sistemas de Información (ASSI).

La acreditación será concedida en base a unas determinadas condiciones de seguridad de la Información clasificada, tanto en lo referente a la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), como a la Seguridad en el Personal, la Seguridad Física de las instalaciones y la Seguridad de la Información, que deberán ser previamente acreditadas, y de las que el solicitante deberá aportar las evidencias documentales necesarias para su valoración y aprobación, en todo caso se ajustará a lo establecido en la normativa sobre seguridad de la información en los sistemas de información y telecomunicaciones que esté en vigor en el Ministerio de Defensa.

La acreditación tiene un carácter temporal, por lo que deberá renovarse siempre que transcurra su plazo de validez o que se produzcan cambios que supongan una modificación apreciable de las condiciones de seguridad.

Serán objeto de Acreditación específica, por un lado, los Sistemas dedicados al manejo de Información clasificada (típicamente estaciones aisladas, redes de área local y redes de área extensa), y por otro, las interconexiones entre dos o más de estos Sistemas.

Para cada Sistema e interconexión de Sistemas se emitirá, una vez aprobadas sus condiciones seguridad (Seguridad de la Información – documental -, Seguridad en el Personal, Seguridad Física - de las instalaciones - y Seguridad en los Sistemas), el correspondiente Certificado de Acreditación.

Todo proceso de Acreditación de Sistemas se regirá por las siguientes fases:

Fase 1.- Inicio del proceso de Acreditación:

La empresa que desee acreditar sus sistemas CIS, presentará por escrito solicitud a la DGAM (SDGINSERT)–acompañado de la documentación acreditativa de estar en posesión de HSEM y HSES. Además, deberá incluir una descripción del Sistema a acreditar, que se ajustará al formato de Concepto de Operación definido en el anexo XVIII.

Una vez aprobada la documentación aportada, se comunicará este hecho a la empresa.

Fase 2.- Elaboración y aprobación de la documentación de seguridad:

La empresa, una vez aprobado el Concepto de Operación, elaborará el resto de documentación de seguridad exigida en cada caso.

Dicha documentación, junto con aquella complementaria que en su caso se pueda solicitar para acreditar la certificación con que cuente el personal y los locales del Sistema, deberá ser enviada igualmente para su aprobación.

Fase 3.- Implementación del Sistema y de su entorno de seguridad:

Una vez aprobada la documentación de seguridad del Sistema, la empresa podrá ponerlo en funcionamiento, de acuerdo a dicha documentación y a las condiciones de seguridad especificadas en ella.

La empresa comunicará a la DGAM (SDGINSERT), con antelación suficiente, la fecha a partir de la cual el Sistema y su entorno de seguridad (entornos de seguridad local, global y electrónico) estarán listos para su inspección, a fin de que esta última pueda comunicarlo al Organismo que ha de efectuarla.

Fase 4.- Inspección del Sistema y de su entorno de seguridad:

El Sistema a autorizar será inspeccionado por el Órgano competente a fin de verificar su correcta implementación, de acuerdo a la documentación de seguridad aprobada.

El resultado de dicha inspección será comunicado oficialmente a la empresa. Aun resultando positiva la evaluación realizada, ésta no constituye en sí una autorización al Sistema para operar, la cual será comunicada oficialmente por escrito, una vez verificado el resto de condicionantes (seguridad física, seguridad en el personal y seguridad documental).

Fase 5.- Acreditación:

Tras la verificación positiva de las condiciones de seguridad del Sistema (seguridad documental, seguridad física, seguridad en el personal y seguridad técnica), se emitirá del correspondiente Certificado de Acreditación, el cual constituye, a todos los efectos, la única autorización para que el Sistema maneje Información clasificada.

Fase 6.- Explotación del Sistema

Una vez obtenido el Certificado de Acreditación, se deberán mantener las condiciones de seguridad iniciales que dieron lugar a dicha autorización. En caso contrario, este Certificado de Acreditación pierde automáticamente toda validez, siendo imprescindible la superación de un proceso de reacreditación, destinado a la obtención de un nuevo Certificado de Acreditación del Sistema.

Con el fin de verificar que los Sistemas autorizados para el manejo de Información clasificada mantienen las condiciones de seguridad que dieron lugar a la Acreditación, éstos se someterán a un proceso de inspecciones de seguridad periódicas.

Fase 7.- Reacreditación

Transcurrido el periodo de validez del Certificado de Acreditación, el Sistema pierde su autorización para manejar Información clasificada. Es responsabilidad de la empresa el iniciar, con la antelación suficiente, los trámites para la reacreditación del mismo.

También son motivo de reacreditación del Sistema los cambios que afecten a sus condiciones de seguridad. Antes de realizar dichos cambios, éstos deben ser

aprobados por el Órgano competente, que verificará el impacto de dichos cambios en las condiciones de seguridad exigidas al sistema.

Fase 8.- Baja del Sistema

Cuando acaba la vida útil de un Sistema autorizado para el manejo de Información clasificada, es responsabilidad de la empresa garantizar la correcta desclasificación de sus activos y la destrucción de la Información clasificada almacenada en él.

Los procedimientos a seguir en este caso estarán recogidos en el Documento de Requisitos de Seguridad del Sistema o interconexión, tal y como se indica en la guía CCN STIC 202.

14. MATERIAS CLASIFICADAS NO NACIONALES

El artículo 11. e) del Decreto 242/69 por el que se desarrollan las disposiciones de la Ley 9/68, sobre Secretos Oficiales, modificada por la 48/78, obliga a la protección de las materias clasificadas entregadas a ESPAÑA por otros países u organismos internacionales.

ESPAÑA tiene firmado una serie de acuerdos bilaterales y multilaterales, en los que se estipulan los procedimientos para proteger las materias clasificadas que se intercambien las partes, o que resulten de programas o consorcios internacionales.

Las condiciones comunes a las citadas normas, de obligado cumplimiento, son las siguientes:

1. No se podrá entregar materia clasificada a terceros, sin el consentimiento previo de la parte originadora de la misma.
2. Cada materia clasificada de la otra parte, recibirá la protección correspondiente a su grado equivalente en ESPAÑA.
3. Nadie podrá acceder a materia clasificada sin la preceptiva Autorización de Acceso concedida por la Autoridad competente.
4. Los países participantes en el programa, proyecto o consorcio internacional determinarán las normas de seguridad que se aplicarán en el mismo.
5. Cuando sea un contratista el custodio de la materia clasificada, estará obligado a cumplir las normas de seguridad determinadas por las Autoridades de los países participantes.
6. Las materias clasificadas proporcionadas por otro país u organismo internacional estarán marcados con la clasificación asignada en origen y con la equivalente en España.

En defecto de norma aplicable para la protección de la materia clasificada entregada por otro país u organismo internacional al Ministerio de Defensa, se aplicará lo dispuesto en estos procedimientos.

15. PROCEDIMIENTO PARA LA SOLICITUD DE INFORMACIÓN SOBRE HSEM/HSES

Cuando un Órgano de Contratación del Ministerio de Defensa precise conocer si una o varias empresas disponen de las habilitaciones necesarias para participar en un Contrato o Programa, empleará el formulario del anexo XIX, que enviará por fax o correo electrónico a la DGAM (SDGINSERT).

16. GLOSARIO DE TÉRMINOS Y DEFINICIONES

Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC): Autoridad designada por el propietario del Sistema, responsable del desarrollo, la operación y mantenimiento del Sistema durante su ciclo de vida; de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.

Área Clase I: zona en la que se maneja y almacena información clasificada de tal forma que la entrada a la zona supone, a todos los efectos, el acceso a dicha información, por lo que sólo puede acceder personal debidamente habilitado y autorizado.

Área Clase II: zona en la que se maneja y almacena Información clasificada de tal forma que pueda estar protegida del acceso de personas no autorizadas mediante controles establecidos internamente, por lo que se podrá admitir la entrada a personal visitante debidamente controlado.

Certificado de Acreditación de Locales (CAL): reconocimiento o autorización expresa, mediante certificado escrito, de la capacidad de un determinado local, edificio, oficina, habitación u otra área para que en el mismo se pueda almacenar o manejar Información clasificada, en unas condiciones establecidas, constituyéndose como Zona de Acceso Restringido configurada como Área Clase I ó Área Clase II, y que especifica los tipos y grado máximo de clasificación de la Información clasificada que puede ser almacenada o manejada en la misma.

Certificado de Inspección y Cumplimiento: certificado con el que se hace declaración expresa de que las medidas de seguridad establecidas en el Plan de Protección son acordes a dicho Plan.

Cláusula de Seguridad: requisitos que se incluyen en un pliego de cláusulas administrativas particulares de un contrato sobre las medidas a adoptar y a exigir a un contratista para manejar información.

Comunicación de Contrato Clasificado: documento por el se declara o comunica a la empresa contratista la clasificación de un contrato.

Compromiso de Seguridad: es el acto por el que se firma el documento de su mismo nombre que obliga al contratista formalmente a proteger la Información clasificada que genere o maneje en razón de la ejecución de una actividad, contrato o programa clasificado, conforme a los requisitos exigidos por la normativa de protección de la Información clasificada en vigor, así como a recibir inspecciones periódicas y a devolver la Información clasificada que le ha sido entregada.

Concepto de Operación: Declaración expresa que realiza la AOSTIC sobre el objeto o función del Sistema, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación, etc.) y las amenazas a las que estará sometido.

Correo: Persona encargada de la transmisión o transporte de Información clasificada.

Criptocustodio: Responsable de la administración y custodia del material de Cifra existente en una cuenta de Cifra asegurando su correcta transmisión y evitando su pérdida.

Cuenta Cifra/Cripto: término para referirse a un Órgano de Control que maneja y/o almacena información clasificada del tipo Cifra.

Ficha del contratista: ficha resumen de características de un contratista que va a solicitar una HSEM.

Diligencia de Clasificación: documento por el que la autoridad facultada aprueba la propuesta de clasificación de la información.

Directiva de Clasificación: 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.

Disponibilidad: requisito básico de seguridad que garantiza que se puede acceder a la información y a los recursos o servicios que la manejan, conforme a las especificaciones de los mismos.

Equivalencia con una HSEM o HSES: reconocimiento formal a una empresa extranjera de que tiene la capacidad y fiabilidad previstas para una HSEM o HSES, respectivamente.

Guía de Clasificación: documento que recoge los datos relevantes de la información clasificada (los grados de clasificación asignados a la misma, las vigencias de las clasificaciones, las autoridades facultadas que la han clasificado, etc.), y que sirve de referencia para el marcado de los documentos.

Habilitación de Seguridad de Empresa (HSEM): reconocimiento formal de la capacidad y fiabilidad de un contratista para generar y acceder a Información clasificada hasta un determinado grado, sin que pueda manejarla o almacenarla en sus propias instalaciones.

Habilitación de Seguridad de Establecimiento (HSES): reconocimiento formal de la capacidad y fiabilidad de un contratista poseedor de una HSEM para manejar y almacenar Información clasificada hasta un determinado grado en aquellas de sus propias instalaciones habilitadas al efecto.

Habilitación Personal de Seguridad (HPS): reconocimiento formal de la fiabilidad de una persona para tener acceso a Información clasificada, en el ámbito o ámbitos y grado máximo autorizado, que se indiquen expresamente, al haber superado el oportuno proceso de acreditación de seguridad y haber sido adecuadamente concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento.

Información: concepto abstracto e intangible que se elabora, presenta, almacena, procesa, transporta o destruye mediante elementos tangibles.

Información de USO OFICIAL: información no clasificada cuya distribución esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo.

Información de USO PÚBLICO: información no clasificada cuya distribución NO esté limitada.

Instalación: se entenderá por instalación de una empresa la oficina, local, edificio o grupo de edificios pertenecientes a la empresa, en una misma localización geográfica, dentro de un perímetro claramente definido.

Instrucción de Seguridad de Programa: requisitos que se incluyen en un Programa sobre las medidas a adoptar y a exigir a un contratista para manejar información.

Integridad: requisito básico de seguridad que garantiza que la información no pueda ser o no ha sido modificada o alterada por personas, entidades o procesos no autorizados.

Órgano de Control: término designado para referirse de manera general al conjunto de personal, recursos materiales y procedimientos que, actuando coordinadamente, tienen como finalidad proteger la Información clasificada del grado y tipo correspondiente. Se clasifican por orden de importancia en Servicio Central de Protección de Materias Clasificadas (SCPMC), en Servicio General de Protección de Materias Clasificadas (SGPMC), en Servicio Local de Protección de Materias Clasificadas (SLPMC).

Plan de Protección: documento que recoge el conjunto de medidas encaminadas a dar evidencia objetiva de que las medidas de seguridad implantadas, tanto de seguridad física, como de seguridad en el personal y de la información, junto con los procedimientos organizativos de seguridad, de obligado cumplimiento, constituyen un entorno de seguridad definido, estudiado y adaptado a la normativa vigente, que permite el manejo o almacenamiento seguro de la Información clasificada así como la protección de los objetivos definidos de un contrato o programa con el MINISDEF.

Plan de Transporte: Documento que describe las distintas medidas de seguridad bajo las que se desarrollará y protegerá un transporte de Información clasificada que sea de un tamaño, peso o cualquier otra característica que aconseje su transporte como mercancía.

Propuesta de Clasificación: documento por el que se somete, a la autoridad facultada para clasificar, la propuesta de asignación de grado de clasificación a informaciones individuales o agrupadas en un conjunto, así como su vigencia, de acuerdo con el procedimiento de reclasificación que regulará la variación temporal del grado asignado.

Propuesta de Guía de Clasificación: documento que se hace para elaborar la Guía de Clasificación.

Servicio de Protección (SP): Servicio previsto por el contratista que está formado por el conjunto de personal, instalaciones, recursos materiales y procedimientos que, actuando coordinadamente, tienen como finalidad proteger la Información clasificada en poder de dicho contratista, de los accesos no autorizados a la misma, y de la pérdida de su integridad y disponibilidad.

Sistemas de Información y Comunicaciones (CIS): Sistemas de Transmisión de la Información clasificada procesada o almacenada que debe protegerse contra la pérdida de confidencialidad, integridad y disponibilidad, sea accidental o intencionada.

Vocal técnico de seguridad: persona designada por un Órgano de Contratación, para representar a éste en una mesa de contratación en los aspectos relacionados con la seguridad de la información.

Zona de Acceso Restringido (ZAR): área en la que se va a manejar y/o almacenar información clasificada, que deberá contar con las medidas y procedimientos de seguridad adecuados y suficientes para asegurar la protección de dicha información en todo momento.

Madrid, 23 de septiembre de 2013

EL DIRECTOR GENERAL DE ARMAMENTO Y MATERIAL

Juan Manuel García Montaño

17. ANEXOS

ANEXO 0: COMPROMISO DE SEGURIDAD

	OFICINA NACIONAL DE SEGURIDAD	
	Seguridad Industrial	

COMPROMISO DE SEGURIDAD

D/Dª. ……, con D.N.I. nº……, en calidad de apoderado de la empresa ……..,.con CIF …….. (en adelante "el Contratista"), según poder que le ha sido conferido ante el Notario de ……Don/Dña. ……bajo el número……de su Protocolo con fecha ……./……./…… .

Considerando que el Contratista está interesado en participar en contratos que impliquen el acceso a:

- Información Clasificada nacional, así como Información Clasificada cuyo manejo y protección se encuentren regulados por tratados internacionales de carácter bilateral o multilateral en virtud del artículo 11 apartado e) del Decreto 242/1969, de 20 de febrero sobre Secretos Oficiales,

Y teniendo en cuenta las disposiciones contenidas en la Ley 9/68, de 5 de abril, reguladora de los Secretos Oficiales, en el Decreto 242/1969, de 20 de Febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y en el Código Penal español,

SE COMPROMETE A CUMPLIR DILIGENTEMENTE LAS SIGUIENTES OBLIGACIONES Y ESTIPULACIONES:

CLÁUSULA PRIMERA – PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA.

a) El Contratista se obliga a implantar y mantener una estructura de protección dentro de su organización, para salvaguardar la Información Clasificada de acuerdo con las exigencias de las NORMAS DE SEGURIDAD DE LA ANS-D, y demás reglamentos de seguridad aplicables, cuyos contenidos conozco y asumo. Dicha estructura de protección será aprobada y periódicamente revisada por la ANS-D.

b) El Contratista se compromete a manejar y custodiar la Información Clasificada exclusivamente en las Zonas de Acceso Restringido especialmente habilitadas para ello y aprobadas según las citadas NORMAS DE SEGURIDAD DE LA ANS-D.

c) El Contratista se compromete a exigir la Habilitación Personal de Seguridad apropiada a toda persona que deba acceder a la Información Clasificada de que es responsable.

d) El Contratista se compromete a exigir a todo Subcontratista, antes de facilitarle Información Clasificada, que tenga concedido una habilitación de seguridad en consonancia con lo dispuesto en las NORMAS DE SEGURIDAD DE LA ANS-D

CLÁUSULA SEGUNDA – HABILITACIÓN DE SEGURIDAD DE EMPRESA.

a) La firma del presente Compromiso de Seguridad es condición necesaria para la concesión al Contratista de una Habilitación de Seguridad de Empresa, que lo habilite para manejar Información Clasificada.

b) El grado de seguridad otorgado al Contratista podrá quedar temporalmente en suspenso cuando concurran circunstancias que puedan afectar negativamente a la protección de la Información Clasificada. Dicha suspensión requerirá notificación por parte de la ANS-D.

CLÁUSULA TERCERA – INSPECCIONES.

El Contratista se compromete a facilitar las inspecciones que la ANS-D estime necesarias para la comprobación del cumplimiento de las obligaciones y deberes que contrae con la firma del presente Compromiso. Si como consecuencia de dichas inspecciones, la ANS-D determinara que los métodos y normas de seguridad del Contratista no satisfacen lo prescrito, el Contratista será notificado por escrito de tales extremos, a los efectos, de su correspondiente subsanación en los términos que se establezcan en la notificación.

CLÁUSULA CUARTA –INCUMPLIMIENTO.

a) El Contratista asume que el incumplimiento de las obligaciones que aparecen recogidas en las NORMAS DE SEGURIDAD DE LA ANS-D, una vez haya sido previamente advertido por la ANS-D, y comprobado por ésta que las subsanaciones a que se refiere la Cláusula Tercera no han sido llevadas a cabo, podrá determinar la retirada de La Habilitación de Seguridad de Empresa otorgada, inhabilitándole para su participación en contratos/programas clasificados.

b) El Contratista asume que el incumplimiento de la normativa detectado en alguno de sus empleados, podrá determinar la retirada de la Habilitación Personal de Seguridad de dicho empleado, sin perjuicio de otras responsabilidades que se pudieran derivar.

CLÁUSULA QUINTA – DEVOLUCIÓN DE LA INFORMACIÓN CLASIFICADA.

El Contratista se compromete a devolver cualquier Información Clasificada facilitada o generada con ocasión del cumplimiento de los contratos clasificados o durante el desarrollo de programas clasificados, o con motivo de procesos precontractuales, previo expreso requerimiento por escrito de la ANS-D.

CLÁUSULA SEXTA – COSTES.

La firma de este Compromiso de Seguridad no implica responsabilidad de la Administración en los gastos del Contratista que se produzcan con motivo del mismo, o como consecuencia del cumplimiento de las obligaciones aquí señaladas.

EL CONTRATISTA SE OBLIGA A NO UTILIZAR CON FINES PUBLICITARIOS LA EXISTENCIA DEL PRESENTE COMPROMISO DE SEGURIDAD O DE LAS HABILITACIONES DE SEGURIDAD DE SU EMPRESA O DE SUS EMPLEADOS.

En fe de lo cual, se firma el presente Compromiso de Seguridad, en , a de de .

Por el Contratista,

Fdo.

ACUSE DE RECIBO

D/Dª. ……,con D.N.I. nº……,en calidad de apoderado de la empresa ……., con CIF …….. (en adelante "el Contratista"), según poder que le ha sido conferido ante el Notario de ……Don/Dña. ……bajo el número……de su Protocolo con fecha ……/……/…… MANIFIESTA:

Haber recibido un ejemplar de las NORMAS DE SEGURIDAD DE LA ANS-D.

Por el Contratista, RECIBÍ

ANEXO I.- JUSTIFICACIÓN DE LA NECESIDAD DE HSEM/HSES

Siendo de interés para este Órgano de Contratación/ Servicio Proponente/ Oficina de Programa, el que la empresa ……., con CIF núm. …… y sede social en ……. pueda participar en el programa …….. clasificado con el grado de …… , conforme a lo establecido en el artículo 21, punto 2 de la Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad, se considera necesario que la referida empresa tenga concedida la Habilitación de Seguridad de Empresa (HSEM) en dicho grado*.(y, en caso de tener que manejar y/o almacenar Información Clasificada en sus instalaciones, Habilitación de Seguridad de Establecimiento (HSES)).*

En _____, a __ de _____ de _____

(Firmado: El Jefe del Órgano de Contratación, Servicio Proponente u Oficina de Programa)

ANEXO II.- FORMULARIOS PARA SOLICITUD DE HPS

Disponibles en:

http://www.cni.es/es/ons/documentacion/formularios/

Formulario HPS:

- http://www.cni.es/comun/recursos/descargas/Solicitud_HPS.pdf
-
- http://www.cni.es/comun/recursos/descargas/Declaracion_Personal_de_Seguridad.pdf

  http://www.cni.es/comun/recursos/descargas/Propuesta_de_Personal.pdf

Instrucciones para el solicitante.pdf

http://www.cni.es/comun/recursos/descargas/OR-ASIP-02-01_02_Confeccion_Solicitud_HPS.pdf

Concienciación para solicitud de HPS - DECÁLOGO de Protección.pdf

http://www.cni.es/comun/recursos/descargas/Concienciacion_para_solicitud_de_HPS_-_DECALOGO_de_Proteccion.pdf

ANEXO III.- TEXTO DEL ACTA NOTARIAL DE RENUNCIA

D./Dª ……..……., mayor de edad, de nacionalidad …… con domicilio en……..…….…… y titular del Documento Nacional de Identidad / pasaporte nº ……., actuando en calidad de …… en la Empresa ……..., con CIF nº ……., domiciliada en ……, considerando que la Empresa está interesada en participar en contratos que impliquen el acceso a:

- Información Clasificada nacional, así como Información Clasificada cuyo manejo y protección se encuentren regulados por tratados internacionales de carácter bilateral o multilateral en virtud del artículo 11 apartado e) del Decreto 242/1969, de 20 de febrero, sobre Secretos Oficiales,

Y teniendo en cuenta las disposiciones contenidas en la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales, el Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, la ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y el Código Penal español,

Por medio del presente documento **RENUNCIA** formalmente

- A tener acceso, en todo o en parte, a la información anteriormente referida, cualquiera que sea el medio o soporte en que se encuentre.

Fdo.

ANEXO IV.- TEXTO DEL APODERAMIENTO PARA LA FIRMA DEL COMPROMISO DE SEGURIDAD

Se confiere y otorga Poder Especial, pero en su especialidad tan amplio y bastante como en derecho se requiera y sea menester, a favor de D. ……..…… , mayor de edad, para que, por sí solo, en nombre y representación de la Sociedad poderdante, pueda firmar ante la Autoridad Nacional de Seguridad con el mismo, y al efecto de realizar los actos, gestiones y diligencias que sean necesarios o estime convenientes, suscribiendo, aparte de dicho acuerdo, cuantos documentos, tanto públicos como privados, instancias, solicitudes, etc. se requieran o precisen, así como obligarse a lo que sea necesario o conveniente, todo ello sin excepción alguna, en especial en todo lo referente al Compromiso de Seguridad.

ANEXO V.- FICHA DEL CONTRATISTA

Disponible en:

http://www.cni.es/comun/recursos/descargas/Ficha_del_Contratista.pdf

ANEXO VI.- CERTIFICADO DE ACREDITACIÓN DE HSEM/HSES

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

CERTIFICADO DE HABILITACIÓN DE SEGURIDAD DE EMPRESA Y/O ESTABLECIMIENTO

De acuerdo con la información facilitada por la Autoridad Nacional de Seguridad Delegada,

SE CERTIFICA QUE:

La empresa ……,
con CIF nº……y sede social en…….
……..……..……..……..……
dispone / no dispone de las habilitaciones que se indican:

Habilitación de Seguridad de Empresa (HSEM) en grado……..……..……

Habilitación de Seguridad de Establecimiento (HSES) en grado ……..……

Esta certificación es válida a los solos efectos de su presentación por la empresa solicitante en relación con el

Contrato/Expediente nº……,
Título……..……..
Promovido por ……..……

El Subdirector General de Inspección y Servicios Técnicos

MADRID, a ..... de ..... de .....

(Firma y Sello)

ANEXO VII: MODELO DE COMUNICACIÓN DE CONTRATO

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

GRADO DE SEGURIDAD DEL CONTRATO

Denominación:	Número/Referencia:
Diligencia de Clasificación:	
Autoridad de Clasificación:	

GRADO DE SEGURIDAD GLOBAL

El Contratista, por la firma realizada en este formulario, se da por enterado del grado de seguridad asignado, parcial y globalmente, al contrato correspondiente; relacionándose al dorso y en ..... hojas anexas a este documento, las materias clasificadas que se le confían, responsabilizándose de las mismas mediante el correspondiente RECIBO DE MATERIAS CLASIFICADAS (ANEXO IX), que se adjunta.

Contratista u Organismo:	
Domicilio social:	C.I.F.:
Representante del Contratista:	
Cargo:	DNI.:
ÓRGANO RESPONSABLE DEL CONTRATO U OFICINA DE PROGRAMA: Domicilio del Órgano: Jefe del Órgano:	

En .....a.....de..... de .....

En representación del Contratista,
(Sello)

En representación del Ministerio de Defensa,
(Sello)

Fdo.

Fdo.:

GRADO DE SEGURIDAD DEL CONTRATO	
DENOMINACIÓN DEL CONTRATO:	
Nº DE EXPEDIENTE:	GRADO DE SEGURIDAD GLOBAL:
PARTES O ELEMENTOS DIFERENCIABLES	
Especificación: Grado de Clasificación:	
Especificación: Grado de Clasificación:	
Especificación: Grado de Clasificación:	
Especificación: Grado de Clasificación:	
Especificación: Grado de Clasificación:	
Especificación: Grado de Clasificación:	

En .....a.....de..... de .....

En representación del Contratista,
(Sello)

En representación del Ministerio de Defensa,
(Sello)

Fdo.:

Fdo.

ANEXO VIII.- AUTORIZACIÓN DE ACCESO A MATERIAS CLASIFICADAS

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

ACCESO A MATERIAS CLASIFICADAS

I. SOLICITUD

Contratista:

C.I.F.:

Con Habilitación de Seguridad de Empresa concedida en fecha , solicita AUTORIZACIÓN DE ACCESO, para el personal del Apartado II, a las materias clasificadas del Ministerio de Defensa, que a continuación se especifican:

CONTRATO/EXPEDIENTE	CLASIFICACIÓN	IDENTIFICACIÓN DE LAS MATERIAS CLASIFICADAS

El Jefe del Servicio de Protección:
(Fecha, firma y sello)

Fdo.:

II. PERSONA PARA LA QUE SE SOLICITA EL ACCESO

Nombre y apellidos: DNI/Pasaporte:
Nacionalidad:
Grado de la Habilitación Personal de Seguridad: Fecha de caducidad:
Empleo/Cargo:
Fechas para las que se solicita el acceso: De a
Motivo por el que se solicita el acceso:

III. SOLICITUD DE VERIFICACIÓN DE HABILITACIÓN PERSONAL DE SEGURIDAD

Nombre: DNI:

En calidad de Jefe del Órgano Responsable del Programa/Contrato indicado en el apartado I,

Solicita a la Dirección General de Armamento y Material verifique que la persona indicada en el apartado II dispone de la Habilitación necesaria para acceder a la información clasificada del contrato señalado en dicho apartado.

(Firma y sello)

IV. VERIFICACIÓN DE HABILITACIÓN PERSONAL DE SEGURIDAD

De acuerdo con la información suministrada por la Oficina Nacional de Seguridad, la persona indicada en el apartado II dispone de Habilitación Personal de Seguridad suficiente para acceder a las materias clasificadas descritas en el Apartado I.

DGAM (SDG INSERT),
(Fecha, firma y sello)

Fdo.: .....

V. AUTORIZACIÓN DE ACCESO

Nombre: DNI:

En calidad de Jefe del Órgano Responsable del Programa/Contrato:
Número de expediente: de fecha:
Grado de Clasificación::

A la vista de que la persona indicada en el apartado II reúne las condiciones requeridas para el acceso a información clasificada

AUTORIZA SU ACCESO a las materias clasificadas descritas en el Apartado I.

(Firma y sello)

FECHA DE ENVÍO AL CONTRATISTA/ ORGANISMO SOLICITANTE:
VI. CONOCIMIENTO DEL AUTORIZADO
Declaro conocer la clasificación de las materias a las que me ha sido autorizado el acceso. EL AUTORIZADO
FECHA DE COMIENZO DEL ACCESO:
VII. DEVOLUCIÓN
En fecha , El Jefe del Servicio de Protección del contratista devuelve esta Autorización de Acceso al Órgano de Contratación u Oficina de Programa, una vez concluido el motivo que la originó. El Jefe del Servicio de Protección: (firma y sello) Fdo.:

ANEXO IX. RECIBO DE MATERIAS CLASIFICADAS

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

RECIBO DE MATERIAS CLASIFICADAS

DESCRIPCIÓN DE LAS MATERIAS CLASIFICADAS	GRADO DE CLASIFICACIÓN
DATOS DEL REMITENTE	
Nombre y apellidos: Cargo/empleo: Organismo/Empresa: Domicilio:	DNI: C.I.F.:
DATOS DEL DESTINATARIO	
Nombre y apellidos: Cargo/empleo: Organismo/Empresa: Domicilio:	DNI: C.I.F.:
FECHA DE ENTREGA:	HORA:

ANEXO X.- AUTORIZACIÓN PARA TRANSMITIR O REPRODUCIR MATERIAS CLASIFICADAS

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

AUTORIZACIÓN PARA REPRODUCIR O TRANSMITIR MATERIAS CLASIFICADAS

Nombre:

DNI:

En calidad de responsable de la Oficina del Programa/Contrato:

Número de expediente: Grado de Seguridad global:
según Diligencia de Clasificación: de fecha: o, en su caso, actuando como Inspector de Seguridad nombrado para dicho Contrato, otorga AUTORIZACIÓN PARA REPRODUCIR/TRANSMITIR las siguientes materias clasificadas, conforme a los procedimientos establecidos por el Ministerio de Defensa para la Protección de las Materias Clasificadas, al Contratista/Organismo:
C.I.F.:

1. MATERIAS CLASIFICADAS		
DESCRIPCIÓN Y SOPORTE	GRADO DE CLASIFICACIÓN	COPIAS
2. MEDIO DE TRANSMISIÓN		

En....., a ..... de ..... de .....
(Firma y Sello)

ANEXO XI.- MODELO DE ACTA DE DESTRUCCIÓN DE MATERIAS CLASIFICADAS

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

ACTA DE DESTRUCCIÓN DE MATERIAS CLASIFICADAS

DATOS DEL CONTRATISTA U ORGANISMO	
Denominación: C.I.F.:	
Nombre y apellidos del empleado autorizado del Contratista:	DNI.:
Nombre y apellidos del Jefe del Servicio de Protección:	DNI.:

En....., a ..... de ..... de ....., y en presencia de los abajo firmantes, se procede a la destrucción efectiva autorizada por el Ministerio de Defensa con fecha . . . . . de las materias clasificadas que a continuación se citan (utilizar los anexos necesarios):

Nº de registro	**Fecha**	**Descripción del material**	**Clasificación**	**Método destrucción**

Y para que conste, firman la presente Acta en el lugar y fecha que se indica:

El Responsable del Órgano de Control: (Firma y Sello) Fdo.:.	El testigo (con HPS de grado adecuado): Fdo.:. . . . .

ANEXO XII.- LISTA DE PERSONAL AUTORIZADO CON ACCESO A LA ZONA DE ACCESO RESTRINGIDO

Identificación de la ZAR: _____

- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....

ANEXO XIII.- FORMULARIO DE SOLICITUD DE INFORMACIÓN SOBRE LA HABILITACIÓN DE UNA PERSONA, PARA UNA VISITA

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

SOLICITUD

EMPRESA SOLICITANTE:

……

JEFE DE SEGURIDAD DEL SERVICIO DE PROTECCIÓN:

……..

Se ruega proporcionar información sobre la HPS de la persona mencionada abajo

Información	
1. Nombre Completo:	
2. DNI/Nº Pasaporte:	
3. Fecha y Lugar de Nacimiento:	/ /
4. Nacionalidad:	
5. Empleado por: Dirección:	
6. Justificación de la solicitud:	

RESPUESTA

1. Se informa de que la persona indicada:
   - ☐ Está en posesión de HPS de grado:
   - ☐ No está en posesión de HPS

MADRID, a ..... de ..... de .....

(Firma y Sello)

ANEXO XIV.- FORMULARIOS DE SOLICITUD DE VISITA INTERNACIONAL

Formato de solicitud de visitas internacionales, disponible en:

http://www.cni.es/comun/recursos/descargas/Formato_estandar_de_solicitud_de_visitas_internacionales_xSI-RFV-01x.pdf

Formato de solicitud de visitas internacionales en inglés (RFV) disponible en:

http://www.cni.es/comun/recursos/descargas/Formato_abreviado_de_solicitud_de_visitas_en_ingles_xSI-RFVLOI-02bisx.pdf

ANEXO XV. INFORME DE VISITAS

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

INFORME DE VISITAS

1. DATOS DE IDENTIFICACIÓN DEL VISITANTE	
Apellidos:	Nombre:
Nacionalidad:	Pasaporte:
Profesión:	Cargo/Empleo:
Empresa/Organismo:	
Dirección profesional:	Teléfonos/Fax:

2. DATOS DEL CONTRATISTA VISITADO	
Empresa u Organismo:	
Domicilio:	
C.I.F.:	Teléfono/Fax:

3. DATOS RELATIVOS A LA VISITA	
Objeto detallado de la visita:	
Instalaciones visitadas:	
Visita realizada a iniciativa de:	
En nombre propio o representación de:	
Fecha de comienzo:	Fecha de terminación:
Personal del Contratista que participa:	

4. INFORMACIÓN CLASIFICADA A LA QUE EL VISITANTE HA TENIDO ACCESO		
CONTRATO/EXPTE.	CLASIFICACIÓN	IDENTIFICACIÓN DE LA INFORMACIÓN

5. INFORME DEL JEFE DEL SERVICIO DE PROTECCIÓN

Nombre:…….CON DNI:
, presenta el siguiente informe sobre la visita recibida:

En . . . . . ., a . . . . . de . . . . . de . . . . . .
(Firma y sello)

ANEXO XVI.- CERTIFICADO DE CORREO

MINISTERIO DE DEFENSA	DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL SUBDIRECCIÓN GENERAL DE INSPECCIÓN Y SERVICIOS TÉCNICOS

CERTIFICADO DE CORREO

Don:
Empleo/Cargo:
Organismo:
Domicilio: Teléfono/Fax:

en representación del Ministerio de Defensa, otorga ACREDITACIÓN DE CORREO para transportar información clasificada a favor de:

1. IDENTIFICACIÓN DEL PORTADOR

Nombre y apellidos:
D.N.I./Pasaporte:
Empresa u Organismo:
C.I.F.:
Domicilio:
Teléfono: Fax:

2. CARACTERÍSTICAS DE ENVÍO

3. ITINERARIO

Desde:
A:
A través de:
Fecha de inicio: Fecha de finalización:
Paradas previstas:

En ....., a ..... de ..... de .....

El Jefe del Servicio de Protección:
(Di las instrucciones)

El Representante del MINISDEF.:
(Firma y sello)

Fdo.: .....

Fdo.: .....

4. INSTRUCCIONES PARA PASO DE ADUANAS

El correo, si fuere requerido por los funcionarios de Aduanas, presentará la acreditación de correo y su documentación personal, haciendo constar que transporta materias clasificadas, señalando los bultos o pliegos de que sea portador.
En caso de fundadas sospechas de fraude, la Aduana procederá al reconocimiento de los paquetes o pliegos, previo aviso y en presencia de persona autorizada por el Ministerio de Defensa.
La inspección se realizará en lugar cubierto, fuera de la vista de personas no afectadas.
La inspección no podrá extenderse a la lectura, toma de notas o cualquier otra operación que no sea la simple comprobación aduanera.
En caso de apertura, se extenderá por duplicado un acta que será firmado por el funcionario de Aduanas y por el correo, entregándose un acta a cada firmante.
Una vez acabada la inspección se precintará el envío por la Aduana, y el hecho se hará constar en el acta.
Se solicita de los responsables de Aduanas, Policía y/o responsables de Inmigración de los países de entrada, tránsito o salida, su colaboración, caso de ser necesaria, para asegurar una entrega segura del envío clasificado.

5. FINALIZACIÓN DE LA MISIÓN

Declaro que durante el viaje no he sido consciente de ninguna acción realizada por terceros, que hubiera podido afectar a la seguridad de la información que me ha sido encomendada. (En caso contrario, adjuntar informe).

VºBº
El Jefe del Servicio de Protección:

El interesado:

Fdo.: .....

Fdo.: .....

Fecha de devolución al Organismo emisor:

ANEXO XVII.- RECIBO DE TRANSPORTE DE MATERIAL CLASIFICADO

	RECIBO DE TRANSPORTE DE MATERIAL CLASIFICADO		DE : **(Órgano de Control que envía)**	PARA *: **(Órgano de Control que recibe)**
	Número:	**Fecha:**		
	Pág,s Recibo:	**Clasificación Máxima:**		
	Modo de Transporte:			
Destinatario(s) e instrucciones de tramitación y entrega:			Autorizado **(Firma y sello oficial)** Nombre y Apell,s: Cargo o puesto:	Recibido **(Firma, fecha y sello oficial)** Nombre y Apell,s: Cargo o puesto:

Registro Serv. Protección		**IDENTIFICACIÓN DEL MATERIAL CLASIFICADO (DOCUMENTO, EQUIPO, PIEZA, ETC.)**						
Número Registro Central	**Núm. Registro de Órgano Emisor**	**NÚM. / REFERENCIA**	**Fecha**	**Clasificación**	**Idioma**	**ASUNTO / DESCRIPCIÓN (Observaciones)**	**EJEMPLARES**	
							Cantidad	Numeración

*** El Órgano de Control indicado en "PARA:" es responsable de devolver firmado este recibo al Órgano indicado en "DE:" (vía correo postal, e-mail, fax, u otra)**

ANEXO XVIII.- DOCUMENTACIÓN DE SEGURIDAD PARA SISTEMAS CIS

En este anexo se hace mención a distintas normas STIC aprobadas por el Centro Criptológico Nacional (CCN), organismo dependiente del Centro Nacional de Inteligencia (CNI), que es el responsable de la acreditación de los sistemas CIS.

Puede consultar estas normas en el siguiente enlace:

https://www.ccn-cert.cni.es/

Todo Sistema que maneje información clasificada deberá tener actualizada la siguiente documentación de seguridad:

	SECRETO/RESERVADO o equivalente	CONFIDENCIAL o equivalente	DIFUSIÓN LIMITADA o equivalente
Declaración de Requisitos de Seguridad Comunes (DRSC)	Sí	Sí	Sí
Declaración de Requisitos de Seguridad de la Interconexión (DRSI)	Sí	Sí	Sí
Análisis de riesgos	Formal	No Formal	No Formal
Concepto de Operación (CO)	Sí	Sí	Sí
Declaración de Requisitos Específicos de Seguridad (DRES)	Sí	Sí	Opcional
Procedimientos Operativos de Seguridad (POS)	Sí	Sí	Sí
Documento abreviado CO/DRES/POS	"RESERVADO o equivalente"	Sí	Sí
Certificado de Acreditación de Zonas de Acceso Restringido	Sí	Sí	No *
Certificación ZONING de locales	Sí	Sí	No
Certificación TEMPEST de equipamiento	Sí	Sí	No
Certificado de Acreditación	Sí	Sí	Sí

* En empresas contratistas y entidades fuera de la Administración y Fuerzas armadas, sí se requerirá.

La Declaración de Requisitos de Seguridad Comunes (DRSC) es un documento sólo exigido cuando existe un conjunto de Sistemas interconectados (un Sistema de Sistemas), o cuando la complejidad y extensión del Sistema así lo requieran. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

La Declaración de Requisitos de Seguridad de la Interconexión (DRSI) se redactará cuando se requiera interconectar varios Sistemas Autorizados. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

El Análisis de Riesgos se ajustará a la metodología descrita en la guía CCN-STIC 410.

El documento de Concepto de Operación (CO) se ajustará al modelo definido en la guía CCN-STIC 207.

El documento de Declaración de Requisitos de Seguridad (DRES) se ajustará al modelo definido en la guía CCN-STIC 202.

El documento de Procedimientos Operativos de Seguridad (POS) se ajustará al modelo definido en la guía CCN-STIC 203.

Sólo en los casos que en que se cumplan todos y cada uno de los criterios relacionados a continuación, podrán reemplazarse los documentos CO, DRES y POS por un único documento abreviado CO/DRES/POS (definido en la guía CCN-STIC 204):

Equipos aislados o pequeñas redes (máximo 1 servidor y 10 estaciones), y que manejen información clasificada de grado "RESERVADO" o inferior, y que estén ubicados dentro del mismo Entorno Global de Seguridad, y que trabajen en el modo seguro de operación "Unificado al Nivel Superior" o "Dedicado".

ANEXO XIX. SOLICITUD DE INFORMACIÓN SOBRE HSEM/HSES

MINISTERIO DE DEFENSA	**DGAM - SDGINSERT** **Fax: 91 270 47 46** **Tel.: 91 270 47 31 / 72 / 73 / 74** **mailto:seguridad_industrial@oc.mde.es**

CONSULTA SOBRE HABILITACIÓN DE SEGURIDAD DE EMPRESA/ESTABLECIMIENTO

I.DATOS IDENTIFICATIVOS DEL EXPEDIENTE

Expediente Nº: ……

Denominación: ……

Órgano de contratación: ……

Persona de contacto: ……

Tel.: …….. Fax: ……

Autoridad de Clasificación: ……

Fecha de la Diligencia de Clasificación: ……

Grado de Clasificación del Expediente: ……

☐ **Secreto** ☐ **Reservado** ☐ **Confidencial** ☐ **Difusión limitada**

II. DATOS SOBRE LAS EMPRESAS

A cumplimentar por el Órgano de Contratación		A cumplimentar por SDGINSERT				
EMPRESA		HSEM Conforme al Grado del expediente		HSES Conforme al Grado del expediente		OBSERVACIONES
C.I.F.	DENOMINACIÓN SOCIAL	SI	NO	SI	NO	

Por el Órgano de Contratación

Por la Subdirección General de Inspección y Servicios Técnicos
El Subdirector General

(Firma y Sello)

Fdo.:

(Firma y Sello)

Fdo.: