I. — DISPOSICIONES GENERALES

NORMAS

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 Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, tiene como objeto alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa.

Para alcanzar dicho objetivo, la citada política de seguridad establece unos principios básicos y unos criterios estratégicos comunes a todos los ámbitos del Departamento y el desarrollo de un cuerpo normativo sobre seguridad de la información, enmarcando cada conjunto de normas en distintos niveles por amplitud del aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

El primer nivel de desarrollo se corresponde con la citada Orden Ministerial 76/2006, de 19 de mayo, en la que designa como Director de Seguridad de la Información al Secretario de Estado de Defensa, encomendándole que vele por el cumplimiento de la política de seguridad de la información y defina su estructura funcional, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas.

La referida Orden Ministerial 76/2006, de 19 de mayo, establece también, que la seguridad de la información se divide en cinco áreas, atendiendo al elemento tangible que hace uso de ella, siendo una de ellas el Área de Seguridad de la Información del Ministerio de Defensa en poder de las empresas (SEGINFOEMP).

La SEGINFOEMP entiende de las medidas adoptadas en el Departamento y las dirigidas a las empresas y aplicables a ellas, como consecuencia de su participación en programas, proyectos o contratos del Ministerio de Defensa, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Ministerio.

El segundo nivel normativo está formado por un conjunto de normas que desarrollan y detallan la política de seguridad, abarcando un área, subárea o aspecto determinado de la seguridad de la información, siendo su ámbito de aplicación todo el Departamento. Estas normas se fundamentan en los principios básicos de la seguridad de la información recogidos en la Orden Ministerial 76/2006, de 19 de mayo.

La Orden Ministerial 76/2006, de 19 de mayo, consideraba desarrollada esta normativa de segundo nivel por la OMC 17/2001, de 29 de enero, por la que se aprueba el Manual para la Protección de materias Clasificadas del Ministerio de Defensa en poder de las empresas y la OMC 44/2001, de 27 de febrero, por la que se aprueba la normativa para la aplicación de dicho Manual, y por la Orden Ministerial 81/2001, de 20 de abril, por la que se aprueban las normas de protección de contratos del Ministerio de Defensa.

En la referida OMC 17/2001, de 29 de enero, se definía el Acuerdo de Seguridad como el compromiso que asume voluntariamente el Contratista ante el Ministerio de Defensa, por el cual se obliga al exacto cumplimiento de las disposiciones del manual de protección de materias clasificadas del Ministerio de Defensa en poder de empresas.

Ahora bien, por un lado, la Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad, en su artículo 21, exige que las empresas que vayan a acceder a información clasificada con motivo de la contratación en estos ámbitos, han de estar en posesión de la correspondiente Habilitación de Seguridad de Empresa y, en su caso, Habilitación de Seguridad de Establecimiento, siendo preceptivo, acorde a la disposición adicional quinta de dicha Ley, tener en cuenta las disposiciones reglamentarias que dicte la Autoridad Nacional de Seguridad de la Información Clasificada originada por las partes del Tratado del Atlántico Norte, por la Unión Europea y por la Unión Europea Occidental. Y por otro lado, la Orden DEF/2524/2012, de 8 de noviembre, por la que se adecúan las normas y medidas de protección de la información del Ministerio de Defensa en poder de las empresas deroga las mencionadas OMC 17/2001 y 44/2001, por lo que, en consecuencia, resulta derogado el Acuerdo de Seguridad contemplado en ellas.

CVE: BOD-2013-134-15907

La referida Orden Ministerial 81/2001, de 20 de abril, se cita en la política de seguridad de la información del Ministerio de Defensa como parte integrante del desarrollo de segundo nivel de la seguridad de la información en poder de las empresas, y por tanto, debe continuar formando parte de este segundo nivel de seguridad de la información del Departamento.

La Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa, designa al Director General de Armamento y Material como responsable del Área de Seguridad de la Información en poder de las empresas del nivel corporativo, asignándole, entre otras, las funciones de elaborar y mantener la normativa, planes, programas y procedimientos relativos a seguridad de la información en poder de las empresas.

De todo lo anteriormente expuesto, se deduce la necesidad de publicar esta Instrucción, al objeto de desarrollar y complementar el segundo nivel normativo de la política de la seguridad de la información del Ministerio de Defensa en poder de las empresas y actualizar las medidas de protección de esta información para las empresas que participen en programas, proyectos o contratos del Ministerio de Defensa.

La disposición adicional única de la Orden DEF/2524/2012, de 8 de noviembre, por la que se adecúan las normas y medidas de protección de la información del Ministerio de Defensa en poder de las empresas, dispone que la Secretaría de Estado procederá al desarrollo de las normas de «Seguridad de la Información en poder de las empresas», adecuadas a la Ley 24/2011, de 1 de agosto y a la Orden Ministerial 76/2006, de 19 de mayo.

En su virtud,

DISPONGO:

Apartado único. *Aprobación.*

Se aprueban las Normas de Seguridad de la Información del Ministerio de Defensa en poder de las empresas, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Cuentas de cifra.*

En relación con las cuentas de cifra se mantendrá la estructura actual hasta que se apruebe la normativa que regule la gestión del material de cifra del Ministerio de Defensa.

Disposición transitoria segunda. *Regularización de los extintos Acuerdos de Seguridad firmados por la Dirección General de Armamento y Material y por los Cuarteles Generales.*

Las empresas que hubiesen firmado con anterioridad a la entrada en vigor de la Orden DEF/2524/2012, de 8 de noviembre, por la que se adecúan las normas y medidas de protección de la información del Ministerio de Defensa en poder de las empresas, el extinto Acuerdo de Seguridad, podrán regularizar su situación para obtener la correspondiente Habilitación de Seguridad de Empresa y, en su caso, la Habilitación de Seguridad de Establecimiento, en un plazo no superior a seis meses a partir de la entrada en vigor de la presente Instrucción, a través de la Dirección General de Armamento y Material.

Disposición transitoria tercera. *Información y contratos de grado SECRETO.*

A la entrada en vigor de la presente Instrucción, se deberá tener en cuenta que aquellas empresas que tuvieran información del Ministerio de Defensa de grado SECRETO entregada por Órganos de Contratación, Servicios Proponentes, Oficinas de Programa o Servicios de Protección de Materias Clasificadas, deberán comunicarlo a la Dirección General de Armamento y Material, en un plazo no superior a un mes a partir de la entrada en vigor de la presente Instrucción, para su posterior retirada y destrucción, en su caso.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta Instrucción.

CVE: BOD-2013-134-15908

Disposición final primera. *Desarrollo normativo de tercer nivel.*

Se 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.

Disposición final segunda. *Entrada en vigor.*

La presente instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 17 de junio de 2013.—El Secretario de Estado de Defensa, Pedro Argüelles Salaverría.

CVE: BOD-2013-134-15909

Normas de Seguridad de la Información del Ministerio de Defensa en Poder de las Empresas

Primera. *Objeto.*

Estas normas tienen por objeto desarrollar la política de seguridad de la información del Ministerio de Defensa (MINISDEF). en la parte que se deriva de la participación de empresas en contratos, programas y proyectos que impliquen acceso a la información del MINISDEF Para alcanzar dicho objetivo se establecen:

a) Unas directrices comunes en materia de seguridad de la información en poder de las empresas para todas aquellas que participen en programas, proyectos o contratos del MINISDEF, y

b) La estructura funcional necesaria para su dirección, ejecución y control.

Segunda. *Ámbito de aplicación.*

Estas normas afectan a todo el Departamento y serán de aplicación a todas las empresas que manejen o puedan manejar información del MINISDEF.

Cualquier otra normativa interna que trate algún aspecto de la seguridad de la información del MINISDEF en poder de las empresas deberá emanar de la política de la seguridad de la información del MINISDEF y de lo establecido en esta Instrucción.

Tercera. *La Seguridad de la Información en poder de las empresas (SEGINFOEMP).*

1. Definiciones.

Para facilitar la lectura de la presente Instrucción, se incluyen las definiciones contempladas en la política de seguridad del MINISDEF y en los desarrollos de la referida política, y las que se deben considerar a los efectos de estas normas.

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.

Cuenta Cifra: término para referirse a un Órgano de Control que maneja información clasificada del tipo Cifra.

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

Directiva de Clasificación: normas, instrucciones y procedimientos generales que pueden afectar a las medidas de seguridad para la protección de la información clasificada de un contrato o programa.

CVE: BOD-2013-134-15910

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 Habilitación de Seguridad de Empresa (HSEM) o Habilitación de Seguridad de Establecimiento (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.

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.

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 MINISDEF, o a personas y organismos que desempeñen actividades relacionadas con el mismo.

Información de USO PUBLICO: 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.

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.

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.

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 información clasificada de grado CONFIDENCIAL o superior, y que deberá contar con las medidas y procedimientos de seguridad adecuados y suficientes para asegurar la protección de dicha

CVE: BOD-2013-134-15911

información en todo momento. Para las empresas, la información de grado DIFUSIÓN LIMITADA, también se almacenará en una ZAR.

2. Conceptos Generales.

La SEGINFOEMP está orientada a establecer las medidas, dirigidas tanto a los organismos del MINISDEF como a las empresas, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Departamento manejada o que puedan manejar las empresas, como consecuencia de su participación en programas, proyectos o contratos del MINISDEF.

3. HSEM.

Toda empresa que tenga necesidad de acceder a información clasificada del MINISDEF como consecuencia de su participación en programas, proyectos o contratos con el citado Ministerio, deberá tener concedida una HSEM, o equivalente, de grado igual o superior al de dicha información, así como establecidos y autorizada la apertura de los Órganos de Control correspondientes.

4. HSES.

Toda empresa que teniendo concedida una HSEM tenga necesidad de almacenar en sus instalaciones información clasificada del MINISDEF, como consecuencia de su participación en programas, proyectos o contratos del citado Ministerio, deberá tener concedida una HSES, o equivalente, de grado igual o superior al de dicha información.

Las empresas que tengan concedida la HSEM y la HSES, o equivalente, que vayan a manejar información clasificada en sus instalaciones, deberán establecer los Órganos de Control de información clasificada necesarios y elaborar un Plan de Protección que refleje las medidas de seguridad para la protección de la información del Ministerio de Defensa, que incluirá las Zonas de Acceso Restringido (ZAR).

5. HPS.

El personal de las empresas con HSEM que vaya a acceder a información clasificada de grado CONFIDENCIAL o superior, deberá tener concedida y en vigor la correspondiente HPS. Para el acceso a información de grado DIFUSION LIMITADA no será necesario disponer de la mencionada habilitación pero sí tener «necesidad de conocer» y haber sido formado previamente.

6. Acreditación de los Sistemas de Información y Telecomunicaciones (SIT).

Las empresas que tengan HSES y vayan a manejar información clasificada del MINISDEF en los SIT dentro de sus instalaciones, deberán tener concedida la correspondiente acreditación de los mismos emitida por la autoridad de acreditación competente.

7. Instrucciones de Seguridad de Programa, Cláusulas de Seguridad y Guía de Clasificación.

a) Con el fin de salvaguardar la información clasificada, todo programa, proyecto o contrato clasificado, deberá contar con unos requisitos específicos de seguridad. En el caso de los programas o proyectos, dichos requisitos estarán recogidos en las «Instrucciones de Seguridad del Programa», mientras que, en el caso de los contratos, formarán parte de las «Cláusulas de Seguridad».

b) Las Instrucciones de Seguridad del Programa son una compilación de las diversas normas y procedimientos de seguridad necesarios para su aplicación de forma homogénea en un determinado programa o proyecto. Dichas instrucciones quedarán incorporadas al programa o proyecto y serán objeto de revisión durante las diferentes fases del mismo.

c) Las Cláusulas de Seguridad se basarán en la normativa nacional de protección de información clasificada existente o, en el caso de contratos internacionales, en el acuerdo

CVE: BOD-2013-134-15912

bilateral o multilateral que le sea de aplicación, así como en los acuerdos de implementación firmados al amparo de éstos.

d) Tanto las Instrucciones de Seguridad de Programa como las Cláusulas de Seguridad de los contratos contarán con su Guía de Clasificación, documento que debe contener:

1.º Una descripción sucinta de todas las partes diferenciadas del programa, proyecto o contrato, señalando tanto las clasificadas como las no clasificadas.

2.º El grado de clasificación para cada una de las partes señaladas en el punto anterior.

3.º Las modificaciones previsibles en la clasificación de cada una de las partes según las fases del programa.

4.º La fecha o condiciones para su reclasificación o desclasificación, bien de cada una de las partes o bien del conjunto del programa, proyecto o contrato clasificado.

5.º Observaciones y comentarios que permitan una mayor comprensión de cualquiera de los conceptos de la Guía de Clasificación.

Cuarta. *Estructura funcional de la seguridad de la información del Ministerio de Defensa en poder de las empresas.*

1. Nivel corporativo de la seguridad de la información en poder de las empresas.

1.1. Director de seguridad de la información del MINISDEF.

El Director de la Seguridad de la Información en el MINISDEF (DSIDEF), cargo que recae en el Secretario de Estado de Defensa (SEDEF), dirigirá la seguridad de la información y velará por el cumplimiento de la política de seguridad de la información en el Departamento, conforme a lo establecido en el artículo segundo de la Orden Ministerial 76/2006.

1.2. Responsable del Área de Seguridad de la Información en poder de las empresas.

El Director General de Armamento y Material, como responsable del Área de Seguridad de la Información en poder de las empresas, para el desempeño de sus cometidos contará con un órgano de trabajo perteneciente a la estructura orgánica de la Dirección General de Armamento y Material (DGAM). Además de lo establecido en la Instrucción 41/2010, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del MINISDEF, le corresponden los siguientes cometidos:

a) Tramitar al Secretario de Estado Director del Centro Nacional de Inteligencia (SEDCNI), como Autoridad Delegada para la Seguridad de la Información Clasificada designada por Orden PRE/2130/2009, de 31 de julio, los expedientes de concesión de HSEM y, en su caso, de HSES de aquellas empresas nacionales que pretendan participar en programas, proyectos o contratos clasificados del MINISDEF.

b) Poner en conocimiento del SEDCNI cuando se observe algún incumplimiento de la normativa de seguridad de la información por parte de aquellas empresas que participen en programas, proyectos o contratos clasificados del Ministerio de Defensa.

c) Proponer al SEDCNI, cuando se aprecien circunstancias que así lo aconsejen, la cancelación, modificación, suspensión temporal o reactivación de la HSEM y, en su caso, de la HSES, de las empresas que las tuvieran previamente concedidas.

d) Solicitar al SEDCNI, para su aprobación, las aperturas, cierres o modificaciones de los Órganos de Control, Cuentas de Cifra y las acreditaciones de los SIT correspondientes a empresas nacionales que participen en programas, proyectos o contratos clasificados del MINISDEF.

e) Solicitar al SEDCNI, para su aprobación, los nombramientos de los Jefes de Seguridad y suplentes de los Órganos de Control, así como los Cripto-Custodios, Cripto-Custodios Alternos y los Administradores de Seguridad de los SIT, correspondientes a las empresas nacionales que participen en programas, proyectos o contratos clasificados del MINISDEF.

f) Centralizar y aprobar, en su caso, la tramitación hacia el SEDCNI de los expedientes de solicitud de Habilitaciones Personales de Seguridad (HPS) de las empresas nacionales que participen en programas, proyectos o contratos clasificados del MINISDEF.

CVE: BOD-2013-134-15913

g) Aprobar las solicitudes de visitas y de asistencia a reuniones internacionales en el extranjero en las que se vaya a acceder a información clasificada relacionada con programas, proyectos y contratos del MINISDEF, por parte de personal de las empresas españolas.

h) Aprobar las solicitudes de visitas de personal extranjero a empresas españolas en las que se vaya a acceder a información clasificada del MINISDEF en el marco de un programa, proyecto o contrato promovido por el mismo, para su posterior comunicación a las empresas españolas a visitar.

i) Aprobar y remitir, en su caso, al SEDCNI para su tramitación, los Planes de Transporte de materias clasificadas al extranjero, de las empresas españolas en el marco de programas, proyectos y contratos del MINISDEF.

j) Solicitar información al SEDCNI sobre la concesión de HSEM, HSES y Órganos de Control, para aquellas empresas que puedan participar en programas, proyectos o contratos clasificados del MINISDEF cuyo trámite de obtención no se haya realizado por el propio Departamento.

k) Comunicar a las empresas, la concesión, denegación, reactivación modificación, suspensión temporal o cancelación de todas aquellas HSEM, HSES y Órganos de Control que haya tramitado. En los tres últimos casos, comunicará tal circunstancia a los Jefes de Seguridad de la Información del ámbito respectivo para que, en su caso, procedan, a través del Servicio de Protección de Materias Clasificadas correspondiente, a la retirada de la información clasificada que obre en poder de las empresas.

l) Llevar el registro actualizado de las HSEM, HSES, Órganos de Control y HPS concedidas y denegadas, que hayan sido tramitadas por la DGAM, y aquellas otras comunicadas por el SEDCNI.

m) Informar, a petición de los Organismos del Departamento y a la vista de la información suministrada por el SEDCNI, sobre grado y vigencia de la HSEM, HSES, Órganos de Control y HPS de aquellas empresas que vayan a participar en programas, proyectos o contratos clasificados del, MINISDEF y de las acreditaciones de sus SIT.

n) Custodiar los certificados de HPS del personal de empresas emitidos por el SEDCNI, para su posterior comunicación a las empresas.

o) Retirar de las empresas las comunicaciones de HPS emitidas a favor del personal de las mismas cuando hayan cesado los motivos por las que se emitieron, para la posterior remisión de los Certificados de HPS al SEDCNI.

p) Remitir al SEDCNI los informes sobre incidencias de seguridad recibidos por los Jefes de Seguridad de la Información de los ámbitos respectivos.

q) Interpretar la normativa en el ámbito del Departamento, sobre protección de la información del MINISDEF en poder de las empresas.

r) Tramitar hacia la autoridad de control del material de cifra del MINISDEF las peticiones para el establecimiento de las Cuentas de Cifra de empresas.

s) Formar y concienciar, con el asesoramiento y la participación del CNI, a todos los organismos y empresas implicados en la protección de la información clasificada en poder de las empresas.

t) Elaborar el Inventario Anual de los contratos, proyectos y programas clasificados del MINISDEF en que participen las empresas remitiéndolo antes del 31 de enero siguiente, al SEDCNI.

u) Remitir al SEDCNI, copia de la Guía de Clasificación y de las Instrucciones de Seguridad del Programa o de las Cláusulas de Seguridad del contrato.

v) Participar, a requerimiento del SEDCNI, en las inspecciones extraordinarias a los Órganos de Control de aquellas empresas que estén participando en programas, proyectos o contratos clasificados del MINISDEF.

w) Realizar las inspecciones ordinarias a los Órganos de Control de aquellas empresas que participen en programas, proyectos o contratos clasificados del MINISDEF.

x) Coordinar y conformar el Informe Anual del Estado de la Seguridad de la información del MINISDEF en poder de las empresas.

y) Asesorar a las empresas sobre el sistema de protección que deben implantar y realizar la inspección inicial de la/las Zonas de Acceso Restringido (ZAR) correspondientes a los Órganos de Control propuestos por las empresas.

CVE: BOD-2013-134-15914

z) Emitir para aquellas empresas que hayan solicitado una HSES, el Certificado de Inspección y Cumplimiento referido a las medidas de seguridad especificadas en el Plan de Protección, para su remisión, junto al propio Plan, al SEDCNI, quien emitirá el preceptivo Certificado de Acreditación de Locales (CAL).

2. Nivel Específico de la Seguridad de la Información en poder de las empresas.

2.1 Jefe de Seguridad de la Información.

El Jefe de Seguridad de la Información será responsable, en relación con la seguridad de la información en poder de las empresas, de los siguientes cometidos en su respectivo ámbito:

a) Relacionarse con el órgano de trabajo de la DGAM, en todo lo relativo a la seguridad de la información en poder de las empresas.
b) Comunicar a la DGAM la formalización de los contratos, proyectos y programas clasificados, así como las modificaciones que se produzcan en los mismos.
c) Elevar a la DGAM, las propuestas de clasificación de la información para los grados SECRETO y RESERVADO, con ocasión de un programa, proyecto o contrato del MINISDEF.
d) Remitir a la DGAM no más tarde del 15 de enero de cada año, el Inventario Anual de los contratos, proyectos y programas clasificados del año anterior en que participen empresas.
e) Para todos los contratos o expedientes de contratación clasificados será responsable de:

1.º Tramitar la solicitud justificada para la clasificación del expediente de un programa, proyecto o contrato que implique manejo de información clasificada que se reciba de los Órganos de Contratación, Servicios Proponentes u Oficinas de Programa de su ámbito.
2.º Remitir copia de la Diligencia de Clasificación y la Guía de Clasificación, una vez aprobada, al Órgano de Contratación, Servicio Proponente u Oficina de Programa.
3.º Comprobar que los requisitos de seguridad específicos del contrato que han de asumir las empresas, están incluidos en las cláusulas administrativas particulares del mismo.
4.º Tramitar hacia la DGAM las Instrucciones de Seguridad del Programa o Cláusulas de Seguridad recibidas de los diferentes Órganos de Contratación, Servicios Proponentes u Oficinas de Programa, así como las Guías de Clasificación aprobadas.
5.º Comunicar a la DGAM cualquier circunstancia que estime pueda comprometer la seguridad de la información relativa a los contratos o expedientes de contratación.
6.º Establecer el sistema de registro de la información clasificada en poder de las empresas.
7.º Realizar las inspecciones ordinarias de la documentación que sea correspondiente a un programa o contrato generado en su ámbito específico.
8.º Elaborar el Informe anual de Seguridad de la Información en poder de las empresas en lo que se refiere a las responsabilidades atribuidas en las presentes normas.

f) Comunicar a la DGAM y a las empresas contratistas implicadas el Representante para la Seguridad de la Información de un contrato o programa.
g) Asesorar a los Órganos de Contratación, Servicios Proponentes y Oficinas de Programa, en la confección de las Instrucciones de Seguridad de Programa y de las Cláusulas de Seguridad de los contratos o proyectos, a petición de estos.
h) Elevar para su aprobación, por la autoridad de su ámbito, o en quien delegue oficialmente esta atribución, las propuestas justificadas de clasificación de información de grado CONFIDENCIAL Y DIFUSIÓN LIMITADA.
i) Proponer para su aprobación, por la autoridad de su ámbito o en quien delegue oficialmente esta atribución, las Instrucciones de Seguridad del Programa de carácter nacional, remitidas por los Jefes de Programas, Órganos de Contratación o Servicios Proponentes.

CVE: BOD-2013-134-15915

j) Establecer las medidas de seguridad relativas a los contratos o expedientes de contratación con grado DIFUSION LIMITADA y de USO OFICIAL en el ámbito de su competencia.

2.2 Jefe del Área de Seguridad de la Información en poder de las empresas de un ámbito específico.

Dependiendo funcionalmente del Jefe de Seguridad de la Información de su ámbito específico, será responsable de los cometidos que éste le delegue.

2.3 Órganos de Contratación, Servicios Proponentes u Oficinas de Programa.

Serán responsables, en relación con la Seguridad de la Información en poder de las empresas, de los siguientes cometidos:

a) Elaborar y tramitar hacia el Jefe de Seguridad de la Información de su ámbito específico la solicitud justificada para la clasificación de todo expediente que implique manejo de información clasificada, junto con la propuesta de Guía de Clasificación.

b) Incluir, cuando sea preciso, en el pliego de cláusulas administrativas particulares de los contratos la exigencia de la HSEM, HSES en su caso, y el Órgano de Control, así como las condiciones de seguridad necesarias.

c) Elaborar y mantener actualizadas las Instrucciones de Seguridad del Programa, las Cláusulas de Seguridad del contrato y la Guía de Clasificación, para lo cual realizará las siguientes acciones:

1.º En caso de existir una clasificación previa, por Directiva de Clasificación, por Ley o por existir una Diligencia de Clasificación de la materia a clasificar, y de estar conforme con la documentación remitida, dará su informe positivo al Jefe de Seguridad de la Información de su ámbito específico.

2.º Si entre la materia a clasificar hubiera alguna que no estuviese clasificada, tramitará, en caso de no existir objeción alguna, la propuesta de Guía de Clasificación junto con la solicitud de clasificación debidamente justificada, directamente al Jefe de Seguridad de la Información de su ámbito específico, para su tramitación, según procedimiento existente, a la correspondiente autoridad facultada para clasificar.

3.º La entrega a la empresa de información clasificada, relativa a proyectos, programas y contratos clasificados sólo podrá realizarse una vez aprobada la Guía de Clasificación y siempre se realizará a través del Servicio de Protección de Materias Clasificadas correspondiente del MINISDEF.

4.º Remitir las propuestas de Instrucciones de Seguridad del Programa al Jefe de Seguridad de la Información de su ámbito específico.

d) Participar en el ámbito internacional, en la elaboración de las Instrucciones de Seguridad del Programa, así como verificar que se cumplen una vez aprobadas.

e) Proporcionar a la empresa la justificación de la necesidad de que obtenga una HSEM, y, en su caso, una HSES o modifique las que ya tuviera concedidas, con ocasión de algún contrato, proyecto o programa clasificado del MINISDEF.

f) Designar, dentro del ámbito de sus competencias, vocal técnico de seguridad de la información en las empresas, para que forme parte de las mesas de contratación de contratos clasificados del MINISDEF.

g) Informar al Jefe de Seguridad de la Información de su ámbito específico y a la empresa contratista, de la clasificación global asignada al contrato y la específica de las partes que lo integran, así como de las modificaciones que se produjeran.

h) Comunicar al Jefe de Seguridad de la Información de su ámbito específico, la designación del Representante para la Seguridad de un Contrato/Programa.

i) Registrar y tramitar, a través de su Servicio de Protección de Materias Clasificadas, la información clasificada que se vaya a entregar a la empresa contratista.

j) Informar al Jefe de Seguridad de la Información de su ámbito específico sobre la necesidad de que la empresa solicite o modifique su HSEM y, en su caso, su HSES.

CVE: BOD-2013-134-15916

k) Registrar y tramitar hacia el Jefe de Seguridad de la Información de su ámbito específico la formalización de contratos o programas clasificados, así como sus modificaciones.

l) Verificar que se cumplen las condiciones de seguridad requeridas antes de autorizar la subcontratación que implique el acceso a información clasificada.

m) Autorizar a los Órganos de Control de las empresas, a través del Servicio de Protección de Materias Clasificadas correspondiente, la realización de reproducciones, transmisiones y destrucciones de copias de la información clasificada del contrato o programa.

n) Informar, al Servicio de Protección de Materias Clasificadas, para que proceda a retirar la información clasificada que obre en poder de la empresa contratista, a la finalización, no adjudicación o suspensión del contrato, o en el caso de suspensión o cancelación de la HSEM o de la HSES.

o) Comunicar al Jefe de Seguridad de la Información de su nivel específico cualquier circunstancia que estime pueda comprometer la seguridad de la información clasificada relativa al contrato o expediente de contratación.

p) Elaborar el Inventario de la información clasificada que durante el año anterior se haya recibido o entregado a los distintos contratistas, y remitirlo al Jefe de Seguridad de la Información de su ámbito específico antes del 31 de diciembre de cada año.

q) Garantizar que todo programa, proyecto o contrato que implique el acceso a información clasificada lleve anexo los siguientes documentos:

— Instrucción de Seguridad del Programa o Cláusulas de Seguridad.
— Guía de Clasificación.
— Comunicación de Clasificación del Contrato.

2.4 Representante del Ministerio de Defensa para la seguridad de la información del Departamento en poder de las empresas. Inspector de Seguridad.

a) Será nombrado por el Director General de Armamento y Material con la denominación de Inspector de Seguridad. El nombramiento se hará efectivo cuando la empresa acceda a un programa, proyecto o contrato clasificado del Ministerio de Defensa, produciéndose el cese a la finalización del mismo.

b) Representará al MINISDEF ante la empresa, durante la ejecución de un contrato clasificado, en los aspectos relativos a la seguridad de la información del Departamento.

c) Controlará el marcado de la información clasificada que genere o reproduzca la empresa previa autorización del órgano responsable del contrato o programa.

d) Velará por el cumplimiento, en el ámbito industrial y tecnológico, de lo establecido en las correspondientes Instrucciones de Seguridad de los Programas y Clausulas 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 sistema de protección de la empresa.

e) Certificará la necesidad que tienen los empleados de la empresa de solicitar HPS, en relación a la función que desempeñan o puedan desempeñar, firmando en su caso la solicitud de Habilitación Personal de Seguridad.

f) Deberá recibir la correspondiente formación para el desempeño de sus cometidos.

2.5 Representante para la Seguridad del Contrato o Programa.

a) Será designado por el Jefe del Programa, Servicio Proponente o, en su defecto, por el Órgano de Contratación responsable de la ejecución del contrato, a los que representará ante el Jefe de Seguridad de la Información en poder de las empresas de su ámbito específico y ante las empresas contratistas.

b) Deberá recibir la correspondiente formación en el manejo de información clasificada y su nombramiento será comunicado, por el Jefe de Seguridad de la Información de su ámbito específico, a la DGAM y a las empresas contratistas implicadas.

c) Los cometidos del Representante para la Seguridad del contrato o programa son:

1.º Velar por el adecuado tratamiento de la información del contrato o programa en poder de la empresa contratista.

CVE: BOD-2013-134-15917

2.º Firmar las autorizaciones de acceso a la información clasificada del personal de la empresa contratista y al personal directamente subcontratado, correspondientes a su contrato o programa, que esté en posesión de la HPS del tipo y grado correspondiente.

3.º Comunicar al Jefe de Seguridad de la Información en poder de las empresas de su ámbito específico cualquier circunstancia que estime pueda comprometer la seguridad de la información del contrato o programa.

4.º Certificar, cuando no haya sido nombrado para un programa, proyecto o contrato clasificado del MINISDEF, Inspector de Seguridad representante del Departamento, la necesidad que tienen los empleados de la empresa contratista y el personal directamente subcontratado, de solicitar HPS, con relación a la función que desempeñan o puedan desempeñar en el contrato, proyecto o programa clasificado, mediante la firma de la solicitud correspondiente.

CVE: BOD-2013-134-15918