I. — DISPOSICIONES GENERALES

MINISTERIO DE DEFENSA

NORMAS

Instrucción 9/2011, de 24 de febrero, del Secretario de Estado de Defensa, por la que se aprueban las normas para la Seguridad de la Información en las Personas.

La Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo, tiene como objeto alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa.

Para alcanzar dicho objetivo, la citada política 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 una única norma que establece principios generales abarcando todo el ámbito de la seguridad de la información, y está constituido por la Política de Seguridad de la Información del Ministerio de Defensa. En esta orden ministerial que aprueba esta política se designa como Director de Seguridad de la Información (DSIDEF) al Secretario de Estado de Defensa.

El segundo nivel es un conjunto de normas que desarrollan y detallan la Política, 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 Política de Seguridad de la Información del Ministerio de Defensa.

Las normas para la aplicación de la Política de Seguridad de la información se recogen en la Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa. En esta instrucción se designa al Director General de Infraestructura como responsable de las Áreas de Seguridad de la Información en las Personas, en los Documentos, en los Sistemas de Información y Telecomunicaciones y en las Instalaciones, atribuyéndole funciones corporativas en estas materias. Para la realización de estas tareas, se designaba como órgano de apoyo técnico a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (IGECIS). Con la entrada en vigor del Real Decreto 1287/2010, de 15 de octubre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, las funciones asignadas en esta materia al desaparecido IGECIS, son ahora responsabilidad de la Subdirección General de Tecnologías de la Información y Comunicaciones, de conformidad con el artículo 6.3.d) de dicho real decreto.

Las presentes normas de seguridad de la información en las personas establecen los requisitos exigidos a las personas para garantizar razonablemente el correcto uso de la información. Se establece, por una parte, el principio de «necesidad de conocer» para limitar el acceso a la información del Ministerio de Defensa sólo a aquellas personas cuyo trabajo lo exige y de otra, la formación en seguridad de la información como paso previo al manejo de la información del Ministerio de Defensa. Además, se desarrolla el concepto de habilitación personal de seguridad, ya introducido en la Política de Seguridad de la Información del Ministerio de Defensa, que certifica, respecto de la persona habilitada, que por las condiciones personales que reúne puede confiársele sin riesgo información clasificada de grado CONFIDENCIAL o superior y que ha sido previamente instruida sobre sus responsabilidades y obligaciones en esta materia.

La disposición final primera de la Orden Ministerial número 76/2006, de 19 de mayo, concede al Secretario de Estado de Defensa facultades para dictar disposiciones de desarrollo y ejecución de dicha orden ministerial.

CVE: BOD-2011-053-6724

En su virtud,

DISPONGO:

Primero. *Aprobación.*

Se aprueban las Normas para la Seguridad de la Información en las Personas, cuyo texto se inserta a continuación.

Disposición derogatoria única. *Derogación normativa.*

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

Disposición final primera. *Desarrollo normativo.*

El desarrollo normativo de la Seguridad de la Información en las Personas se realizará tanto a nivel corporativo como a nivel específico, e incluirá entre otros, los siguientes documentos:

a) A Nivel Corporativo:

1.º Procedimiento para la gestión de la habilitación personal de seguridad de la información en el Ministerio de Defensa.
2.º Plan global y continuo de formación en seguridad de la Información en las personas.
3.º Procedimiento de notificación al DSIDEF del informe anual sobre el estado de la seguridad de la información en las personas, incluyendo la información del registro general de la habilitación personal de seguridad (HPS).
4.º Procedimiento de notificación y respuesta ante incidentes de seguridad de la información en las personas.
5.º Procedimiento de interlocución a nivel corporativo con el CNI en relación a la seguridad de la información en las personas.

b) A Nivel Específico contendrá el procedimiento con la estructura funcional y cometidos del área de Seguridad de la Información en las Personas, siguiendo las directrices emanadas del nivel corporativo.

Disposición final segunda. *Entrada en vigor.*

La presente instrucción entrará en vigor a los nueve meses de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 24 de febrero de 2011.—El Secretario de Estado de Defensa, Constantino Méndez Martínez.

Normas para la Seguridad de la Información en las Personas

Primera. *Objeto.*

Estas normas tienen como objeto desarrollar la Política de Seguridad de la Información del Ministerio de Defensa en todo lo concerniente a las personas.
Para alcanzar dicho objetivo se establecen:

a) Unas directrices comunes en materia de seguridad de la información en las personas en todo el ámbito del Ministerio, y
b) la estructura funcional necesaria para su dirección, ejecución y control.

Segunda. *Ámbito de aplicación.*

Estas normas afectan a todo el Departamento y se aplicarán a todas las personas que manejen o puedan manejar información del Ministerio de Defensa.
Cualquier instrucción interna que trate algún aspecto particular de la seguridad de la información del Ministerio de Defensa en las personas deberá emanar de la Política de la Seguridad de la Información, sus normas de aplicación y de lo establecido en estas normas.

CVE: BOD-2011-053-6725

Tercera. *La seguridad de la información en las personas.*

La seguridad de la información en las personas entiende de los requisitos exigidos a las personas con el objeto de garantizar la confidencialidad, integridad y disponibilidad de la información del Ministerio de Defensa que manejan o puedan manejar (en adelante se utilizará sólo el término manejar). Deberá coordinarse con el resto de áreas: seguridad de la información en los documentos, seguridad de la información en los sistemas de información y telecomunicaciones, seguridad de la información en las instalaciones y seguridad de la información en poder de las empresas.

Las medidas de seguridad a aplicar irán orientadas a disuadir y prevenir los incidentes de seguridad de la información que manejan las personas y, en caso de que estos ocurran, minimizar los daños y adoptar las medidas adecuadas para evitar su repetición.

Cuarta. *Principios básicos.*

Los principios básicos de la seguridad de la información en las personas son:

a) La autorización de acceso personal a la información del Ministerio de Defensa se concederá en base a la necesidad de conocer, derivada del desempeño de sus cometidos oficiales. Todo el personal que vaya a acceder a la información del Ministerio deberá conocer previamente cuáles son sus responsabilidades y obligaciones.

b) Cuando la información esté clasificada con grado CONFIDENCIAL o superior, la autorización de acceso personal se concederá siempre y cuando la persona tenga la necesidad de conocer y disponga de la correspondiente habilitación personal de seguridad (HPS).

Quinta. *Habilitación personal de seguridad.*

1. La Habilitación Personal de Seguridad (HPS) certifica que la persona a quién le ha sido concedida:

a) Reúne unas condiciones personales adecuadas para que se le pueda confiar información del Ministerio de Defensa, clasificada de grado CONFIDENCIAL o superior.

b) Ha sido instruida en materia de seguridad y conoce las responsabilidades penales y disciplinarias en las que pudiera incurrir.

2. La HPS no faculta, por sí sola a su titular, para acceder a toda la información del mismo grado de clasificación o inferior al que ha sido habilitado. Dicho acceso estará condicionado siempre por su necesidad de conocer y por su autorización de acceso.

3. Se definen los siguientes grados de habilitación:

a) «Secreto»: capacita a su titular para acceder a información clasificada de grado SECRETO e inferior.

b) «Reservado»: capacita a su titular para acceder a información clasificada de grado RESERVADO e inferior.

c) «Confidencial» capacita a su titular para acceder a información clasificada de grado CONFIDENCIAL.

4. Podrán establecerse autorizaciones especiales que complementen las habilitaciones personales de seguridad, en el caso de que la naturaleza de la información lo requiera (información relativa a criptología, inteligencia de señales, etc.). Estas autorizaciones especiales irán asociadas a la HPS del solicitante.

Sexta. *Solicitud de la habilitación personal de seguridad.*

1. El solicitante deberá cumplimentar debidamente el cuestionario vigente, conforme al procedimiento establecido por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) dando su autorización expresa para que se lleven a cabo las investigaciones oportunas.

2. El Ministerio de Defensa colaborará con el CNI en las investigaciones, aportando todos aquellos informes sobre el solicitante que le sean requeridos en el ejercicio de esta función.

3. La solicitud de la HPS será tramitada por el Jefe de Seguridad de la Información del ámbito de nivel específico al que pertenezca el solicitante, siguiendo el procedimiento que se establezca para tal fin por el Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF).

CVE: BOD-2011-053-6726

4. El inicio de los trámites de solicitud de la HPS no presupone su concesión y, por tanto, la autorización para acceder a información clasificada deberá quedar supeditada a los resultados obtenidos tras la finalización de este procedimiento.

5. En el caso de que la solicitud sea para la obtención de la HPS de grado CONFIDENCIAL, la Autoridad del ámbito correspondiente podrá autorizar, bajo su responsabilidad el acceso de forma temporal a la información, siempre que se hayan iniciado los trámites para la concesión de la HPS. Esta autorización quedará supeditada a la obtención de la HPS.

Séptima. *Ciclo de vida de las habilitaciones personales de seguridad.*

1. La concesión, denegación, modificación y retirada de habilitaciones personales de seguridad para el acceso a información clasificada de grado CONFIDENCIAL o superior corresponde al Secretario de Estado Director del CNI, siguiendo el procedimiento que sea establecido.

2. El solicitante o titular de la HPS se compromete a informar de aquellas vicisitudes que puedan suponer un cambio en su situación de seguridad respecto a la concesión de la misma. Es decir, cualquier circunstancia posterior al momento de solicitud de la HPS que pueda suponer una modificación en los niveles de riesgo asumidos, por ejemplo: cambio de estado civil, cambio de nacionalidad, estar incurso en un procedimiento penal o administrativo.

3. Los documentos originales de las habilitaciones personales de seguridad concedidas por el Secretario de Estado Director del CNI serán remitidos, según el procedimiento que sea establecido, al Responsable del área de Seguridad de la Información en las Personas, quién los enviará para su custodia a los Jefes de Seguridad de la Información de ámbito específico, que informará de su concesión al titular según el procedimiento que sea establecido.

4. En ningún caso se entregará la HPS al titular. Cuando sea necesario certificar su posesión, el Jefe de Seguridad de la Información de su ámbito específico podrá emitir certificaciones, con su firma, que serán entregadas al titular o remitidas al organismo que lo precise. Estas certificaciones se harán por un plazo de vigencia limitado y por un motivo concreto.

5. El Jefe de Seguridad de la Información que tenga indicios o haya recibido informes desfavorables acerca de una persona que dentro de su ámbito ostenta una HPS, y haya constatado que existen riesgos para la seguridad, deberá adoptar medidas cautelares para impedirle el acceso a la información clasificada, informando a través de su Autoridad al Responsable del área de Seguridad de la Información en las Personas, quien analizará los hechos, y cuando así lo estime oportuno, informará al DSIDEF y solicitará al CNI un nuevo proceso de investigación. En base al resultado de la investigación, el Secretario de Estado Director del CNI podrá, si procede, retirar la HPS.

6. El Jefe de Seguridad de la Información del ámbito correspondiente enviará al Responsable del Área de Seguridad de la Información en las Personas, siguiendo el procedimiento que sea establecido, el documento original de la HPS retirada para su posterior remisión al Secretario de Estado Director del CNI.

Octava. *Vigencia de las habilitaciones personales de seguridad.*

1. Las habilitaciones personales de seguridad al personal del Departamento serán concedidas por un periodo inicial de cinco (5) años. Si al terminar este periodo se sigue manteniendo la necesidad, se solicitará la renovación, concediéndose por periodos de diez (10) años. Para las habilitaciones de grado SECRETO el periodo máximo de renovación será cinco (5) años, siempre siguiendo el procedimiento establecido por el Secretario de Estado Director del CNI.

2. Como requisito previo a cada renovación se rellenarán los correspondientes cuestionarios y se llevarán a cabo las investigaciones oportunas, siguiendo el mismo proceso que una solicitud inicial.

3. El Jefe de Seguridad de la Información deberá disponer de los mecanismos necesarios para garantizar que todo el personal de su ámbito al que le vaya a caducar la HPS, curse la solicitud de renovación con la antelación suficiente. El incumplimiento de estos

CVE: BOD-2011-053-6727

plazos puede conllevar la caducidad de la HPS y, por tanto, la imposibilidad de acceso a determinada información por parte del usuario.

4. En el caso de que exista una causa justificada por la que no se haya podido tramitar la renovación de la HPS, el Secretario de Estado Director del CNI podrá conceder una extensión de la validez de la habilitación existente por seis (6) meses, siempre y cuando se estén llevando a cabo las acciones oportunas para su renovación. Si la HPS que se está renovando es de grado CONFIDENCIAL, podrá ser extendida por la Autoridad del ámbito al que pertenece el solicitante.

5. Aun existiendo la necesidad de conocer, si no se formaliza la renovación de la HPS en el plazo máximo exigido de seis (6) meses, la persona afectada deberá cesar en las actividades para las que se requiera dicha Habilitación.

Novena. *Cambios de destino del personal.*

Cuando una persona con HPS cambie de destino o puesto de trabajo, y esto implique un cambio de dependencia de Jefe de Seguridad de la Información, deberá ponerlo en conocimiento de su anterior Jefe de Seguridad de la Información, con objeto de que el documento original de concesión de la HPS sea remitida a su nuevo responsable.

Décima. *Instrucción específica para la obtención de la HPS.*

Todos los solicitantes de HPS han de declarar por escrito, como requisito previo para su concesión, que han sido debidamente instruidos y entienden plenamente cuáles son sus deberes de reserva respecto a la información clasificada a la que acceden y sus obligaciones básicas, derivados del acceso a la información, así como de las responsabilidades penales y disciplinarias que le son de aplicación en caso de incumplimiento

La renovación de la HPS también llevará implícito la realización de la fase de instrucción en materia de seguridad de la información.

Undécima. *Requisitos de acceso a información del Ministerio de Defensa por organismos externos a éste*.

1. El personal perteneciente a la Administración Pública Española que, por causas justificadas, pueda tener la necesidad de acceder a información clasificada del Ministerio de Defensa, se regirá por el mismo procedimiento que el personal del Ministerio de Defensa.

2. El personal extranjero con reconocida necesidad de conocer que, por razón de su trabajo, deba acceder a información clasificada de grado CONFIDENCIAL o superior del Ministerio de Defensa, deberá estar en posesión de una Habilitación Personal de Seguridad expedida por la Autoridad competente de su nación y reconocida o convalidada por el Secretario de Estado Director del CNI, conforme a los procedimientos que sean establecidos por este último.

El personal extranjero que por razón de su trabajo deba acceder a información DIFUSIÓN LIMITADA o inferior, será suficiente con que tenga reconocida necesidad de conocer, sea conocedora de sus responsabilidades y obtenga la posterior aprobación del DSIDEF o de en quién él delegue.

3. Las empresas o compañías, incluyendo subcontratistas, que trabajen o quieran trabajar para el Ministerio de Defensa, cuyo personal pueda tener acceso a información clasificada de ese Ministerio, deberán cumplir con la regulación específica de su área.

Duodécima. *Autorización de acceso del personal a la información del Ministerio de Defensa en situaciones de emergencias*.

1. Las Autoridades de cada ámbito, bajo su responsabilidad, podrán autorizar por escrito el acceso a información clasificada, hasta grado RESERVADO incluido, durante periodos de guerra o crisis, o en cualquier situación que haya sido declarada de emergencia por una autoridad competente, a aquel personal que no posea HPS, siempre que dicho acceso sea estrictamente necesario y que se tenga constancia de que se le pueda confiar dicha información.

CVE: BOD-2011-053-6728

2. En estas mismas condiciones, podrá autorizar el acceso a información clasificada hasta grado SECRETO incluido, al personal que tenga concedida la HPS de grado RESERVADO.

3. Deberán informar al DSIDEF y al CNI de todas las autorizaciones de emergencia que se concedan, y mantendrán un registro de la información a la que dicho personal accede.

Decimotercera. *Formación en seguridad de la información.*

1. Con el fin de difundir el conocimiento sobre la normativa de Seguridad de la Información en el Departamento y cualquier otro aspecto que el DSIDEF considere oportuno, se elaborará un plan global y continuo de formación en seguridad de la información para todo el personal que maneje información del Ministerio de Defensa.

2. Todo el personal que vaya a manejar información del Ministerio de Defensa deberá recibir, previo a su acceso, la debida formación en seguridad de la información. Los Jefes de Seguridad de la Información de los distintos ámbitos de nivel específico, serán los responsables de que se lleve a cabo la formación en seguridad de la información, para todo el personal a su cargo, bajo las directrices e indicaciones establecidas por el DSIDEF.

3. A la finalización de la formación, el Jefe de Seguridad de la Información emitirá un certificado en el que se especifique su aprovechamiento. En caso de que éste no sea favorable, se deberá repetir la formación con antelación a poder acceder a la información.

4. La Dirección General de Reclutamiento y Enseñanza Militar (DIGEREM) deberá garantizar, en los planes de estudios para la enseñanza militar de formación y perfeccionamiento, la inclusión de las directrices marcadas por el DSIDEF en materia de seguridad de la información.

Decimocuarta. *Provisión de plazas con acceso a información clasificada del Ministerio.*

1. La Dirección General de Personal (DIGENPER) y los Cuarteles Generales deberán tener en cuenta para elaborar las provisiones de destinos y puestos de trabajo, si en ellos se va a manejar o no información clasificada del Ministerio de Defensa y especificar el grado máximo de clasificación de la información que se podrá manejar.

2. El personal que pase destinado a un puesto que implique manejo de información de grado CONFIDENCIAL o superior deberá estar en posesión de la correspondiente HPS o iniciar los trámites para su obtención en un plazo no superior a un mes, a contar desde su incorporación.

3. En el caso de que no se inicien los trámites en el plazo requerido o sea denegada la HPS del peticionario, se le prohibirá el acceso y/o manejo de la información clasificada del MINISDEF, hasta que su situación sea favorable y disponga de la correspondiente HPS. Si esa situación perdurase más de un mes, podría ser causa de cese o traslado del peticionario a otro puesto y/o destino.

Decimoquinta. *Sistema de registro de las habilitaciones personales de seguridad.*

1. El DSIDEF dispondrá de los mecanismos necesarios para conocer y controlar las habilitaciones personales de seguridad existentes. Cuando lo considere necesario, solicitará al Jefe de Seguridad de la Información del ámbito correspondiente la información recogida en su registro general.

2. En cada uno de los ámbitos de nivel específico, el Jefe de Seguridad de la Información, establecerá y mantendrá un registro general actualizado de todas las habilitaciones personales de seguridad del personal de su ámbito. El mencionado registro contendrá información acerca del titular, grado y fecha de emisión de la HPS, periodo de validez de la misma, y sus posteriores renovaciones y/o modificaciones.

3. El Jefe de Seguridad de la Información de cada ámbito deberá remitir al responsable de seguridad de la información en las personas, un informe con la información de su registro, al menos, con carácter anual y siempre que le sea demandado por éste.

CVE: BOD-2011-053-6729

Decimosexta. *Estructura funcional de la seguridad de la información en las personas*.

1. El Nivel Corporativo de la seguridad de la información en las personas, se estructura en:

a) Director de Seguridad de la Información del Ministerio de Defensa.

El DSIDEF dirigirá y velará por el cumplimiento de la seguridad de la información en las personas en el Departamento, conforme a lo establecido en el artículo segundo de 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 y en sus normas de aplicación.

El DSIDEF es también el responsable de aprobar el Plan Global de formación en Seguridad de la Información, que incluya la seguridad de la información en las personas.

b) Responsable de Seguridad de la Información en las Personas.

Al Responsable de Seguridad de la Información en las Personas, en los Documentos, en los Sistemas de Información y Telecomunicaciones y en las Instalaciones le corresponde elaborar la propuesta del Plan Global de formación y concienciación en Seguridad de la Información, así como todos aquellos cometidos que en materia de seguridad de la información en las personas le asigne el DSIDEF, según lo dispuesto en la Instrucción del Secretario de Estado de Defensa 41/2010, de 7 de julio, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa.

2. El Nivel Específico de la Seguridad de la Información en las Personas se estructura en:

a) Jefe de Seguridad de la Información.

El Jefe de Seguridad de la Información de cada ámbito, en relación con la seguridad de la información en las personas, será responsable de:

1.º Elaborar y proponer a su Autoridad la estructura funcional de detalle del área de seguridad de la información en las personas.
2.º Dirigir y controlar la implantación de las medidas de seguridad de la información en las personas.
3.º Coordinar las medidas de seguridad de la información en las personas con los diferentes responsables de la ejecución de la seguridad de la información en las personas.
4.º Tramitar las solicitudes de las habilitaciones personales de seguridad, del personal de su ámbito (emisión, renovación y modificación).
5.º Custodiar las habilitaciones personales de seguridad del personal de su ámbito.
6.º Emitir certificación de concesión de la HPS al personal que lo solicite de manera justificada.
7.º Mantener el Registro General de las habilitaciones personales de seguridad de su ámbito e informar, según el procedimiento que sea establecido.
8.º Investigar los incidentes de seguridad de la información en las personas y notificarlos según el procedimiento establecido.
9.º Comprobar que el personal de su ámbito, como paso previo a la obtención de la correspondiente HPS, ha recibido la instrucción necesaria para su obtención siguiendo las directrices marcadas por el CNI.
10.º Certificar la debida formación en materia de seguridad de la información para todo el personal que deba acceder a información del MINISDEF, según las indicaciones del DSIDEF.
11.º Delegar en el Jefe de Seguridad de la Información en las Personas aquellos cometidos que él considere oportuno en esta materia.

b) Jefe de Seguridad de la Información en las Personas.

El Jefe de Seguridad de la Información en las Personas dependiendo funcionalmente del Jefe de Seguridad de la Información de su nivel específico, será responsable de los cometidos que éste le delegue.

CVE: BOD-2011-053-6730

c) Responsable de Seguridad de la Información de la Unidad, Centro u Organismo (UCO).

Cuando sea necesario, el Jefe de Seguridad de la Información propondrá, a la Autoridad de su ámbito, la designación de un Responsable de Seguridad de la Información de la UCO, que ejecutará las acciones que el Jefe de Seguridad de la Información le asigne en esta materia.

d) Personal del Ministerio de Defensa.

Todo el personal del Ministerio de Defensa que necesite acceder a información del Ministerio de Defensa deberá seguir las indicaciones de su correspondiente Jefe de Seguridad de la Información y la normativa existente en vigor.

CVE: BOD-2011-053-6731