I. — DISPOSICIONES GENERALES

NORMAS

Instrucción 95/2011, de 16 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información en las Instalaciones.

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 la 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. La orden ministerial antes mencionada 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 Orden Ministerial 76/2006, de 19 de mayo.

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 (DIGENIN) 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 designa como su órgano de Apoyo Técnico a la Inspección General del Plan Director CIS del Ministerio de Defensa, actualmente extinta, debido a su integración en la Subdirección General de Tecnologías de la Información y Comunicaciones de la Dirección General de Infraestructura, según lo dispuesto en el artículo 6.3.d) del Real Decreto 1287/2010, de 15 de octubre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa.

Estas normas de Seguridad de la Información en las Instalaciones establecen los requisitos exigidos a las instalaciones que manejan o puedan llegar a manejar información del Ministerio de Defensa, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la misma.

La disposición final primera de la Orden Ministerial número 76/2006, de 19 de mayo, faculta al Secretario de Estado de Defensa a dictar las disposiciones oportunas, en el ámbito de sus competencias, para el desarrollo y ejecución de la política de seguridad de la información del Ministerio de Defensa.

En su virtud,

DISPONGO:

Apartado único. *Aprobación*.

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

CVE: BOD-2011-251-33500

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 Instalaciones 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 el control de acceso a las Instalaciones en las que se maneja información del Ministerio de Defensa: Proceso de Identificación, Autenticación y Autorización.
2.º Requisitos de seguridad para el control de visitas a las Instalaciones.
3.º Requisitos de seguridad para las Zonas de Seguridad.
4.º Procedimiento para la autorización de una Zona de Seguridad.
5.º Procedimiento para el almacenamiento de información clasificada en las instalaciones del Ministerio de Defensa.
6.º Procedimiento de interlocución a nivel corporativo con el Centro Nacional de Inteligencia (CNI) en relación a la Seguridad de la Información en las Instalaciones.
7.º Procedimiento de notificación al Director de Seguridad de la Información (DSIDEF) del informe anual sobre el estado de la Seguridad de la Información en las Instalaciones.
8.º Procedimiento de notificación y respuesta ante incidentes de Seguridad de la Información en las Instalaciones.

b) A nivel específico, contendrá el procedimiento particular del ámbito para el control de acceso en sus instalaciones.

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, 16 de diciembre 2011.—El Secretario de Estado de Defensa, Constantino Méndez Martínez.

Normas para la Seguridad de la Información en las Instalaciones

Primera. *Objeto.*

Estas normas tienen como objeto desarrollar la Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo, en la parte que afecta a las instalaciones. Para alcanzar dicho objetivo se establecen:

a) Unas directrices comunes en materia de Seguridad de la Información en las Instalaciones que puedan manejar o manejen información del Ministerio, y
b) la estructura funcional necesaria para su dirección, ejecución y control.

Segunda. *Ámbito de aplicación.*

Estas normas afectan a todas las instalaciones en las que se maneje o pueda manejarse (en adelante se utilizará sólo el término maneje) información del Ministerio de Defensa, tal y como establece la Política de Seguridad de la Información del Ministerio de Defensa.
El término instalación utilizado en esta normativa engloba cualquier emplazamiento, o parte de él, en el que se maneja información del Ministerio de Defensa.
Las instalaciones de las empresas que manejan información del Ministerio de Defensa se regulan por el desarrollo normativo del Área de Seguridad de la Información en poder de las Empresas, según se establece en la Política de Seguridad de la Información.

CVE: BOD-2011-251-33501

Cualquier otra normativa interna que trate algún aspecto de la Seguridad de la Información del Ministerio de Defensa en las Instalaciones deberá emanar de la Política de la Seguridad de la Información y de lo establecido en las normas que derivan de ella.

Tercera. *La Seguridad de la Información en las Instalaciones.*

La Seguridad de la Información en las Instalaciones entiende de las medidas de protección a aplicar a las instalaciones en las que se maneje información del Ministerio de Defensa con objeto de garantizar los requisitos de confidencialidad, integridad y disponibilidad de la información considerando los daños que produciría la pérdida de alguno de estos requisitos básicos. Debe coordinarse con el resto de áreas: Seguridad de la Información en las Personas, Seguridad de la Información en los Documentos, y Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.

Las medidas de protección a aplicar deben ir orientadas a:

a) Prevenir y detectar los incidentes de Seguridad de la Información en las Instalaciones y, en caso de de que éstos ocurran, minimizar los daños.
b) Ejercer las pertinentes acciones de corrección sobre posibles brechas o violaciones de seguridad.

Cuarta. *Principios básicos de la Seguridad de la Información en las Instalaciones.*

Los principios básicos de la Seguridad de la Información en las Instalaciones son:

a) Principio de proporcionalidad: La Seguridad de la Información en las Instalaciones está orientada a la definición e implantación de las medidas de protección física más eficaces y adecuadas. Estas medidas deberán establecerse a partir de este principio, teniendo en cuenta las características y el volumen de la información a proteger, las potenciales amenazas a las que se encuentre sometida la información, su probabilidad de materialización y el impacto que causarían.
b) Principio de seguridad continua: Con el objeto de garantizar la eficacia y proporcionalidad de las medidas de seguridad, los requisitos de seguridad física deben establecerse, siempre que sea posible, en las fases de planificación y diseño de las dependencias. Una vez implantadas deben revisarse periódicamente para verificar que siguen siendo eficaces. Se deberán disponer los mecanismos necesarios para garantizar que cualquier cambio o modificación en las medidas de seguridad, se hace de forma controlada, garantizando la eficacia de las mismas.
c) Principio de defensa en profundidad: La Seguridad de la Información en las Instalaciones debe basarse en la creación de un conjunto escalonado de medidas de seguridad, coordinadas entre sí, que impidan o retrasen la acción de la amenaza el mayor tiempo posible, al objeto de facilitar la neutralización de dicho incidente por los elementos de reacción que se hayan definido.
d) Principio de segregación: En las áreas en que se maneje información con diferentes grados de clasificación, se deberán cumplir los requisitos más restrictivos y permitir una separación de la información. Para almacenar información del Ministerio de Defensa se podrán emplear áreas que hayan sido autorizadas para manejar información procedente de otros países u organizaciones, siempre y cuando el grado de protección sea igual o superior al requerido para la información del Ministerio y se garantice la separación de las mismas, siguiendo los procedimientos y requisitos de autorización y acceso establecidos.

Quinta. *Manejo de la información en las Instalaciones.*

1. El manejo de información de USO PÚBLICO no requerirá controles específicos en las instalaciones al no estar limitada su distribución.
2. El manejo de información de USO OFICIAL requerirá la aplicación de las medidas necesarias para garantizar que el acceso a la misma sólo está permitido a las personas autorizadas.
3. La información clasificada deberá manejarse en Zonas de Seguridad.

CVE: BOD-2011-251-33502

Sexta. *Zona de Seguridad.*

1. Se entiende por Zona de Seguridad aquella instalación, o parte de ella, con un perímetro definido e identificado, en la que existe un control y unas condiciones de protección específicas, que permitan el manejo de la información clasificada dentro de la misma.

Las Zonas de Seguridad están específicamente constituidas para permitir la protección de la información clasificada. Se clasifican en Zonas de Acceso Restringido y Zonas Administrativas de Protección.

2. Se define Zona de Acceso Restringido aquella área en la que se va a manejar información clasificada de grado CONFIDENCIAL o superior, por lo que deberá contar con las medidas y procedimientos de seguridad adecuados y suficientes para asegurar la protección de dicha información en todo momento.

Una Zona de Acceso Restringido podrá ser clasificada como Área Clase I o Clase II. La clasificación de una Zona de Acceso Restringido en Área Clase I o Clase II vendrá determinada por las condiciones de accesibilidad a la información clasificada dentro de cada área.

La Zona de Acceso Restringido deberá permanecer cerrada y vigilada cuando no esté siendo usada.

3. Área Clase I es aquella en la que por el mero hecho de acceder a ella proporciona acceso a la información manejada y a los recursos allí contenidos.

Debe cumplir los siguientes requisitos:

a) Disponer de un perímetro claramente definido y protegido en el que se controlen todas las entradas y salidas.

b) Disponer de un control de accesos que admita únicamente a aquellas personas debidamente habilitadas y específicamente autorizadas para acceder a dicha área.

c) Que las personas que accedan al área sean previamente informadas sobre el tipo y grado de clasificación de la información manejada en ella.

4. Área Clase II es la Zona de Acceso Restringido en la que se puede impedir por procedimientos y controles internos el acceso no autorizado a la información y a los recursos allí contenidos.

Debe cumplir los siguientes requisitos:

a) Disponer de un perímetro claramente definido y protegido en el que se controlen todas las entradas y salidas.

b) Disponer de un sistema de control de accesos que sólo permita el acceso sin escolta a aquellas personas que tengan autorización específica para acceder a dicho área y la correspondiente habilitación. A todos los demás se les proporcionará escolta o controles internos para prevenir el acceso no autorizado a la información.

5. La Zona Administrativa de Protección es aquella Zona de Seguridad en la que se puede manejar información clasificada de grado máximo DIFUSIÓN LIMITADA.

Debe disponer de un perímetro claramente definido y protegido, en el cual se controlen todas las entradas y salidas de personal, material y vehículos para que sólo se permita el acceso a aquellos que estén previamente autorizados.

Cuando sea necesario, se establecerá una Zona Administrativa de Protección en torno a las Áreas Clase I y Clase II, o en las zonas que conducen a dichas Zonas de Acceso Restringido.

Séptima. *Área Técnicamente Segura.*

El Área Técnicamente Segura es una zona segura en la que se discute información clasificada y que requiere de la protección necesaria y suficiente frente a escuchas externas. Debe cumplir los siguientes requisitos:

a) Estar específicamente identificada.

CVE: BOD-2011-251-33503

b) Disponer de un control de acceso.

c) Ser sometida a revisiones técnicas y físicas determinadas en el desarrollo normativo correspondiente.

d) Permanecer cerrada y vigilada cuando no esté siendo usada.

e) Por regla general no dispondrán de ningún tipo de dispositivo de telefonía o electrónico equipado con partes electroacústicas. En el caso de que deba existir un dispositivo de estas características, será obligatorio que éste se pueda desconectar físicamente previo al tratamiento de la información clasificada.

f) Se mantendrá un registro de todos los equipos o muebles que estén ubicados en su interior o hayan sido retirados del área. No se introducirá en estas zonas ningún mueble o equipo que no haya sido previamente inspeccionado y autorizado por personal de seguridad específicamente formado.

La autorización de un área como Técnicamente Segura es independiente de la posible autorización como Zona de Seguridad.

Octava. *Control de acceso.*

Se deberá controlar el acceso a cualquier instalación en la que se maneje información del Ministerio de Defensa e implantar las medidas necesarias para garantizar que sólo las personas debidamente autorizadas pueden acceder a la información, de acuerdo con lo establecido en la norma quinta.

El acceso se determinará para cada persona de manera individual. La concesión del acceso irá determinada por la necesidad de acceso, por la necesidad de conocer y, cuando sea de aplicación, por la posesión de la correspondiente Habilitación Personal de Seguridad.

Será responsabilidad del Jefe de Seguridad de la Información del ámbito específico definir y establecer el procedimiento para el control de accesos a las instalaciones de su ámbito, que garanticen la correcta identificación, autenticación y autorización de todas las personas que quieren acceder, conforme a los requisitos que a tal efecto apruebe el Director de Seguridad de la Información del Ministerio (DSIDEF). Este procedimiento deberá incluir requisitos para el control de acceso para la entrada y salida con dispositivos móviles, equipos portátiles y en general cualquier documento que contenga o pueda contener información del Ministerio de Defensa.

Novena. *Autorización de seguridad otorgada a una Zona de Seguridad.*

La autorización de seguridad otorgada a una Zona de Seguridad permitirá manejar información clasificada del Ministerio de Defensa en su interior. Dicha autorización se ajustará al procedimiento que para tal fin apruebe el DSIDEF.

Previamente a que en una Zona de Seguridad se maneje información clasificada de grado CONFIDENCIAL o superior, deberá estar autorizada por la autoridad del ámbito de nivel específico al que pertenece la unidad, centro u organismo (UCO). Las autoridades de cada ámbito podrán designar respectivamente un organismo de autorización de apoyo a sus funciones, cuando lo consideren necesario.

Décima. *Sistema de Registro de las Zonas de Acceso Restringido.*

1. El DSIDEF dispondrá de los mecanismos necesarios para conocer y controlar todas las Zonas de Acceso Restringido existentes.

Cuando lo considere necesario, solicitará al Jefe de Seguridad de la Información del ámbito correspondiente, a través de su autoridad, 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 Zonas de Acceso Restringido de su ámbito.

Este registro deberá permitir mantener un inventario de todas las Zonas de Acceso Restringido autorizadas, con indicación del tipo de autorización otorgado, la fecha de caducidad y el Jefe de Seguridad de la Información del que depende la instalación.

CVE: BOD-2011-251-33504

3. El Jefe de Seguridad de la Información de cada ámbito deberá remitir al Responsable del área de Seguridad de la Información en las Instalaciones, a través de su cadena funcional, un informe con la información de su registro, al menos, con carácter anual y siempre que le sea demandado por éste.

Undécima. *Estructura funcional de la Seguridad de la Información en las Instalaciones.*

1. En la estructura funcional de la Seguridad de la Información en las Instalaciones se distinguirá entre el nivel corporativo y el nivel específico.

2. El nivel corporativo de la Seguridad de la Información en las Instalaciones comprende a:

a) El Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF), que dirigirá y velará por el cumplimiento de la seguridad de la Información en las instalaciones en el Departamento, conforme a lo establecido en el artículo segundo de la Orden Ministerial 76/2006, de 19 de mayo, y en sus normas de aplicación.

b) El Responsable del área de Seguridad de la Información en las Instalaciones, al que le corresponden todos aquellos cometidos que, en materia de seguridad de la información en las instalaciones, le asigne el DSIDEF, según lo dispuesto en 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.

3. El nivel específico de la Seguridad de la Información en las Instalaciones comprende a:

a) El Jefe de Seguridad de la Información de cada ámbito, en relación con la Seguridad de la Información en las Instalaciones, que será responsable de:

1.º Dirigir y controlar la implantación de las medidas de Seguridad de la Información en las Instalaciones.

2.º Definir, establecer e implementar los controles internos de seguridad que deben llevarse a cabo para evitar accesos no autorizados a la información existente en sus Instalaciones.

3.º Definir un procedimiento específico para el control de accesos a las Instalaciones de su ámbito.

4.º Velar porque se confeccionen y mantengan las listas de personal, material y vehículos autorizados con acceso a las Zonas de Acceso Restringido.

5.º Coordinar las medidas de Seguridad de la Información en las Instalaciones con los diferentes responsables de la ejecución de la Seguridad de la Información en las Instalaciones.

6.º Mantener el registro general de las Zonas de Acceso Restringido.

7.º Canalizar las solicitudes de autorización de seguridad de las Zonas de Seguridad, según el procedimiento establecido y llevar a cabo la inspección previa.

8.º Recibir y valorar los informes de incidentes de Seguridad de la Información en las Instalaciones, adoptar o proponer las medidas correctoras oportunas y, según lo establecido, informar al DSIDEF a través del jefe o autoridad del ámbito correspondiente.

9.º Promover la formación y concienciación en Seguridad de la Información en las Instalaciones que sea necesaria.

10.º Delegar en el Jefe de Seguridad de la Información en las Instalaciones aquellos cometidos que él considere oportuno en esta materia.

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

c) El 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.

Este responsable solo será designado por la UCO correspondiente cuando sea necesario, tras la propuesta del Jefe de Seguridad de la Información a la autoridad de su ámbito.

CVE: BOD-2011-251-33505

d) Todo el personal que acceda a instalaciones donde se maneje información del Ministerio de Defensa, que deberá seguir las indicaciones del correspondiente Jefe de Seguridad de la Información, del personal en quién él delegue y la normativa en vigor existente.

CVE: BOD-2011-251-33506