V. — OTRAS DISPOSICIONES

NORMAS

Cód. Informático: 2016018296.

Instrucción 53/2016, de 24 de agosto, 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.

El apartado primero de la Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo, establece que es objeto de la misma el «alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa». Para lograr tal objeto, se establecen en dicha política las definiciones, los conceptos y los principios básicos comunes a todos los ámbitos del Departamento. En el apartado segundo de la citada Orden Ministerial, se designa como Director de Seguridad de la Información del Ministerio de Defensa al Secretario de Estado de Defensa y se le encomienda, entre otras funciones, dirigir la seguridad de la información y definir y crear la estructura funcional de la seguridad de la información.

La disposición adicional única.1 de 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, designó 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»; y la disposición adicional única. 3, al Director General de Armamento y Material como «responsable del área de seguridad de la información en poder de las empresas».

Tras la publicación de esta Instrucción se han producido diversos cambios normativos que afectan a la misma.

En primer lugar, el artículo 4.2.i) del Real Decreto 454/2012, de 5 de marzo, atribuye a la Dirección General de Armamento y Material, entre otras funciones, la de ejercer las competencias que le confieren las leyes y reglamentos en materia de Seguridad Industrial relacionada con la defensa.

En segundo lugar, el artículo 15 del Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas, determina que «el Mando Conjunto de Ciberdefensa será responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa». Y su artículo 19, señala que la Unidad Militar de Emergencias es una organización operativa permanente subordinada al Jefe del Estado Mayor de la Defensa.

Así mismo, el artículo 11.2 de la Orden DEF/166/2015, de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas, establece que el Mando Conjunto de Ciberdefensa «será responsable del desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT) y de la dirección de la ejecución y el control del cumplimiento de estas políticas, en el ámbito del Ministerio de Defensa».

En tercer lugar, el artículo 3.3 del Real Decreto 454/2012, de 5 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, tras la modificación operada por el Real Decreto 837/2015, de 21 de septiembre, regula el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, y establece que le corresponde «la planificación y desarrollo de las políticas de los sistemas, tecnologías y seguridad de la información del Departamento, así como la supervisión y dirección de su ejecución».

CVE: BOD-2016-171-21244

Finalmente, se ha establecido la Política de Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC) a través de la Orden DEF/2639/2015, de 3 de diciembre. Uno de los principios de esta Política es la Seguridad en los sistemas y servicios, de manera que la protección de la información no afecte a su tratamiento o transmisión. Uno de sus ejes estratégicos es consolidar la Seguridad en los CIS/TIC, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a ciberataques en línea, entre otros, con la Política de Seguridad de la Información del Ministerio. Por este motivo y para asegurar el alineamiento, la aplicación de la Política de Seguridad de la Información debe ser coherente, además, con los principios, finalidad, ejes estratégicos, directrices y estructura de gobierno establecidos en la citada Política CIS/TIC.

Los cambios normativos que se han expuesto determinan la necesidad de elaborar una nueva Instrucción, que regule las normas para la aplicación de la Política de Seguridad de la Información del Departamento, atribuyendo las responsabilidades en materia de seguridad de la información con arreglo a lo establecido en las disposiciones citadas, con la consiguiente derogación de la Instrucción 41/2010, de 7 de julio.

La disposición final primera de la Orden Ministerial 76/2006, de 19 de mayo, faculta al Secretario de Estado de Defensa para dictar cuantas disposiciones requiera la aplicación de esa orden ministerial.

En su virtud,

D I S P O N G O:

Apartado único. *Aprobación de las Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa*.

Se aprueban las Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada 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.

2. Asimismo, queda derogada cualquier otra disposición de igual o inferior rango que se oponga a lo establecido en esta instrucción.

Disposición final primera. *Facultades dispositivas.*

Las autoridades de los diferentes ámbitos de la estructura funcional de la seguridad de la información que se establece en las normas que aprueba esta Instrucción, así como los responsables de las diferentes áreas de seguridad de la información, podrán dictar, en el ámbito de sus competencias, cuantas disposiciones requiera la aplicación de esta instrucción, que serán coordinadas por el Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones para su presentación al Director de Seguridad de la Información del Ministerio de Defensa.

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, a 24 de agosto de 2016.—El Secretario de Estado de Defensa, Pedro Argüelles Salaverría.

CVE: BOD-2016-171-21245

Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa

CAPITULO I

Disposiciones Generales

Primera. *Finalidad*.

Estas normas tienen por finalidad:

a) Establecer la estructura funcional de la seguridad de la información del Ministerio de Defensa, incluyendo en ella el Servicio de Protección de Materias Clasificadas, así como definir sus respectivas funciones y cometidos.

b) Definir la estructura de gobierno de la seguridad de la información del Ministerio, que permita el seguimiento, coordinación y control de la política en esta materia.

c) Regular el Plan de Actuación para la Seguridad de la Información y su desarrollo mediante Planes de Acción.

Segunda. *Ámbito de aplicación.*

Estas normas son de aplicación en el Ministerio de Defensa, conforme a lo establecido en la Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo.

Tercera. *El Director de Seguridad de la Información del Ministerio de Defensa.*

El Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF) es el Secretario de Estado de Defensa que tiene, entre otras, la función de definir y crear la estructura funcional de la seguridad de la información del Ministerio de Defensa, incluyendo en ella el Servicio de Protección de Materias Clasificadas, con arreglo a lo dispuesto en la disposición segunda 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.

Cuarta. *Plan de Actuación para la Seguridad de la Información y su desarrollo.*

1. Para facilitar el desarrollo de la Política de Seguridad de la Información del Ministerio de Defensa, se elaborará el Plan de Actuación para la Seguridad de la Información, que complementará el desarrollo normativo establecido en el apartado octavo de la Política de Seguridad de la Información, y cuyo objeto y estructura mínima se presenta en el anexo a estas Normas. Su elaboración será responsabilidad del Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), con la colaboración de los Responsables de las Áreas de Seguridad para aquellas partes del Plan relativas a sus respectivas áreas de responsabilidad, y será aprobado por el Secretario de Estado de Defensa.

2. El Plan de Actuación para la Seguridad de la Información se desarrollará a través de los correspondientes planes de acción de las diferentes áreas de seguridad de la información que se definan, según lo reseñado en el anexo a estas Normas.

CAPITULO II

Estructura funcional de la seguridad de la información del Ministerio de Defensa

Quinta. *Estructura funcional de la seguridad de la información.*

Para llevar a cabo la dirección, ejecución y supervisión de la seguridad de la información del Ministerio de Defensa se establecen los siguientes niveles funcionales:

a) Nivel corporativo, que afecta a todo el ámbito del Departamento.

b) Nivel específico, que afecta a cada uno de los ámbitos en que se estructura este nivel.

CVE: BOD-2016-171-21246

Sexta. *Nivel corporativo.*

1. Este nivel es responsable, en el ámbito del Departamento, de la dirección, coordinación, evaluación y supervisión de las medidas de seguridad de la información.

2. Forman parte de este nivel:

a) El DSIDEF, que dirige la seguridad de la información y vela por el cumplimiento de la Política de Seguridad de la Información en el Departamento.
b) El Director del CESTIC, que define, planifica y coordina la Política de Seguridad de la Información del Departamento, dirige su ejecución y controla el cumplimiento de las citadas políticas en el ámbito del Departamento.
c) Los Responsables de las Áreas de Seguridad de la Información, que llevarán a cabo la coordinación y supervisión de la seguridad de la información en sus respectivas áreas. Son los siguientes:

1.º El Director del CESTIC, que será el responsable del Área de Seguridad de la Información en las Personas (SEGINFOPER), asesorado por la Dirección General de Personal en el ámbito de su competencia.
2.º El Secretario General Técnico, que será el responsable del Área de Seguridad de la Información en los Documentos (SEGINFODOC).
3.º El Director General de Infraestructura, que será el responsable del Área de Seguridad de la Información en las Instalaciones (SEGINFOINS).
4.º El Director General de Armamento y Material, que será el responsable del Área de Seguridad de la Información en poder de las Empresas (SEGINFOEMP).
5.º El Comandante Jefe del Mando Conjunto de Ciberdefensa que será el responsable del Área de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT).

Séptima. *Nivel específico.*

1. En el nivel específico se establecen los siguientes ámbitos:

a) El Estado Mayor de la Defensa.
b) La Secretaría de Estado de Defensa, que incluye las unidades y órganos con dependencia directa del Ministro de Defensa.
c) La Subsecretaría de Defensa.
d) El Ejército de Tierra.
e) La Armada.
f) El Ejército del Aire.
g) La Secretaría General de Política de Defensa.

2. En cada uno de los ámbitos establecidos en el apartado anterior habrá un Responsable de Seguridad de la Información, nombrado por la Autoridad del ámbito (Jefe de Estado Mayor de la Defensa, Secretario de Estado de Defensa, Subsecretario de Defensa, Jefe de Estado Mayor del Ejército de Tierra, Jefe de Estado Mayor de la Armada, Jefe de Estado Mayor del Ejército del Aire y Secretario General de Política de Defensa), que llevará a cabo la dirección y coordinación de las medidas de seguridad de la información en todas las áreas de seguridad de la información de su ámbito.

3. En cada uno de estos ámbitos habrá un Jefe de Seguridad de la Información que será responsable de la ejecución y supervisión de las medidas de seguridad de la información en todas las áreas de seguridad de la información dentro de su ámbito específico. Tal y como se establece en la norma undécima, será nombrado por la Autoridad del ámbito a propuesta del Responsable de Seguridad de la Información correspondiente, y tendrá rango mínimo de Jefe de Área, Coronel o Capitán de Navío.

CVE: BOD-2016-171-21247

4. El Responsable de Seguridad de la Información organizará en su ámbito las áreas de seguridad, pudiendo establecer jefes en las diversas áreas que dependerán funcionalmente del Jefe de Seguridad de la Información de su ámbito específico y serán responsables de los cometidos que éste les encomiende en relación con su respectiva área de seguridad de la información.

Octava. *Funciones y cometidos del Director de Seguridad de la Información del Ministerio de Defensa.*

En el ejercicio de las funciones que recoge la norma sexta. 2. a) el DSIDEF tendrá los siguientes cometidos:

a) Convocar y presidir el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa (CDSIDEF), establecido en la Orden Ministerial 76/2006, de 19 de mayo, y recogido en el Capítulo III de estas normas como órgano de la estructura de gobierno de la seguridad de la información.

b) Aprobar el Plan de Actuación para la Seguridad de la Información.

c) Aprobar el Informe Anual de la Seguridad de la Información del Ministerio de Defensa.

d) Aprobar la normativa del segundo nivel de seguridad de la información.

e) Elevar a la autoridad u órgano competente, las propuestas para clasificar, reclasificar o desclasificar materias clasificadas con el grado de RESERVADO o SECRETO.

Novena. *Funciones y cometidos del Director del CESTIC.*

1. Al CESTIC le corresponde la planificación y desarrollo de la Política de Seguridad de la Información del Departamento, así como la supervisión y dirección de su ejecución.

2. En el ejercicio de esta competencia, el DICESTIC tendrá las siguientes funciones:

a) Definir, planificar y coordinar las políticas de seguridad de la información del Departamento.

b) Dirigir la ejecución y controlar el cumplimiento de las citadas políticas en el ámbito común al Departamento.

c) Convocar y presidir la Comisión Ejecutiva de Seguridad de la Información del Ministerio de Defensa (CESIDEF), como órgano de la estructura de gobierno de la seguridad de la información regulado en el Capítulo III de estas normas.

d) Elaborar el Plan de Actuación para la Seguridad de la Información y elevarlo al DSIDEF para su aprobación.

e) Ostentar la representación e interlocución, en lo relativo a la seguridad de la información, ante otros organismos de la Administración del Estado y, en el ámbito internacional, en coordinación con el Estado Mayor de la Defensa y la Dirección General de Política de Defensa. Para el caso concreto de cada una de las áreas de Seguridad de la Información, esta función será llevada a cabo por el responsable del área correspondiente en coordinación con el CESTIC.

f) Estudiar, analizar y evaluar los informes sobre seguridad de la información remitidos por los Responsables de las Áreas de Seguridad de la Información y proponer las medidas correctoras pertinentes al CDSIDEF.

g) Coordinar el desarrollo de la normativa, planes, programas y procedimientos de aplicación en todo el Ministerio de Defensa y divulgarlos, una vez sean aprobados por el DSIDEF.

h) Proporcionar asistencia y apoyo al DSIDEF en las materias de seguridad de la información que éste determine.

i) Examinar y evaluar las propuestas de clasificación, reclasificación y desclasificación de materias clasificadas con grado RESERVADO o SECRETO presentadas al DSIDEF al objeto de elevarlas para su aprobación por la autoridad u órgano facultado para ello.

j) Coordinar con los Responsables de las Áreas de Seguridad de la Información la elaboración de la normativa de tercer nivel de carácter corporativo de sus respectivas áreas para su aprobación y difusión.

CVE: BOD-2016-171-21248

k) Estudiar, analizar, valorar y hacer seguimiento de las nuevas tendencias, avances técnicos y normativos en materia de seguridad de la información, tanto de carácter nacional como internacional, así como consolidar las propuestas de los Responsables de las Áreas de Seguridad de Información en estas cuestiones.

l) Ejecutar aquellas otras acciones que el DSIDEF y el CDSIDEF le asignen en materia de seguridad de la información.

Décima. *Cometidos de los Responsables de las Áreas de Seguridad de la Información.*

1. El responsable de cada una de las áreas de seguridad de la información tendrá, en su ámbito de competencia, los siguientes cometidos a nivel corporativo:

a) Convocar y presidir el Comité de Seguridad de la Información del Ministerio de Defensa de su respectiva área de seguridad, como órgano de la estructura de gobierno de la seguridad de la información regulado en el Capítulo III de estas normas.

b) Coordinar y supervisar la seguridad de la información en el área de la que sea responsable y elaborar el correspondiente Informe Anual del estado de la seguridad de la información, para lo cual tendrá en cuenta los informes remitidos por los diferentes ámbitos del nivel específico. Informes que serán remitidos al DICESTIC quien elaborará un único informe y lo presentará para su aprobación al DSIDEF.

c) Elaborar y desarrollar la normativa, planes, programas y procedimientos corporativos de aplicación en todo el Ministerio de Defensa y presentarlos a la Comisión Ejecutiva de Seguridad de la Información o al Consejo de Dirección de Seguridad de la Información según proceda.

d) Canalizar las propuestas de clasificación, reclasificación y desclasificación de materias clasificadas de grado RESERVADO o SECRETO, procedentes de los ámbitos de nivel específico, y presentarlas al DSIDEF, al objeto de su análisis y posterior aprobación por la autoridad u órgano facultado para ello.

e) Estudiar, analizar, valorar y hacer seguimiento de los avances técnicos y normativos en materia de seguridad de la información en el área de su competencia, tanto de carácter nacional como internacional y proponer medidas para mejorar la seguridad de la información en su área de responsabilidad.

2. Los responsables de las cinco áreas de seguridad de la información, serán responsables del desarrollo y detalle de las Políticas de Seguridad de la Información en su área, y de la dirección de la ejecución y el control del cumplimiento de estas políticas, en el ámbito del Ministerio de Defensa.

3. El responsable de la SEGINFOEMP deberá, además de los cometidos anteriores, velar por el cumplimiento, en el ámbito industrial y tecnológico, de lo establecido en las correspondientes instrucciones sobre seguridad de la información en las empresas.

Undécima. *Cometidos de los Responsables de Seguridad de la Información de los ámbitos del nivel específico.*

El Responsable de Seguridad de la Información de cada uno de los ámbitos del nivel específico tendrá los siguientes cometidos:

a) Dirigir y coordinar la seguridad de la información en su ámbito, de conformidad con las directrices establecidas por el DSIDEF, el CDSIDEF y por los responsables de las áreas de seguridad de la información del nivel corporativo.

b) Proponer a la Autoridad de su ámbito la designación de un Jefe de Seguridad de la Información del ámbito, así como de los respectivos jefes de cada una de las áreas de seguridad de la información que determine, con rango mínimo de Jefe de Área, Coronel o Capitán de Navío.

c) Dirigir la elaboración de la normativa necesaria para adecuar y trasladar a su ámbito específico la normativa de nivel corporativo.

d) Aprobar las directrices, estructura y funcionamiento del Servicio de Protección de Materias Clasificadas de su ámbito.

CVE: BOD-2016-171-21249

Duodécima. *Cometidos de los Jefes de Seguridad de la Información de los ámbitos del nivel específico*.

El Jefe de Seguridad de la Información de cada uno de los ámbitos del nivel específico tendrá los siguientes cometidos:

a) Evaluar la seguridad de la información de su ámbito y elaborar el correspondiente informe anual, que presentará a su autoridad para su remisión al DSIDEF a través de los responsables de las áreas de seguridad de la información del nivel corporativo.

b) Dirigir, implantar y supervisar la ejecución de las medidas de seguridad de la información en su ámbito, de acuerdo con las directrices del Responsable de Seguridad de la Información de su ámbito.

c) Elaborar y proponer al Responsable de Seguridad de la Información de su ámbito, la estructura funcional de seguridad de la información en su ámbito más adecuada a las directrices y normas emanadas del DSIDEF.

d) Dirigir el Servicio de Protección de Materias Clasificadas de su ámbito específico y proponer las directrices, estructura y funcionamiento de dicho servicio a su Responsable de Seguridad de la Información para su aprobación.

e) Elevar las propuestas de clasificación, reclasificación o desclasificación de materias clasificadas CONFIDENCIAL o inferior específicas de su ámbito a su Responsable de Seguridad de la Información para su aprobación por la Autoridad del ámbito.

f) Canalizar las propuestas de clasificación, reclasificación o desclasificación de materias clasificadas RESERVADO o superior en su ámbito a su Responsable de Seguridad de la Información, para su remisión al DSIDEF a través del Responsable del Área de Seguridad de la Información correspondiente.

g) Velar por el cumplimiento de la citada Política de Seguridad de la Información del Ministerio de Defensa y comunicar al responsable de la correspondiente área de seguridad de la información los incidentes de seguridad que, habiendo tenido origen en su ámbito, puedan afectar a todo el Departamento.

h) Elaborar y proponer, para su aprobación por su Responsable de Seguridad de la Información, la normativa, planes, programas y procedimientos de seguridad de la información de su ámbito, siguiendo las directrices marcadas por el DSIDEF.

i) Colaborar con el responsable de la correspondiente área de seguridad de la información en el estudio, análisis, valoración y seguimiento de las nuevas tendencias y de la normativa de seguridad de la información de carácter nacional e internacional.

j) Ejecutar aquellas otras acciones que su Responsable de Seguridad de la Información le asigne en materia de seguridad de la información.

k) Coordinar a los jefes de las Áreas de Seguridad de la Información de su ámbito.

Decimotercera. *Servicio de Protección de Materias Clasificadas*.

El Servicio de Protección de Materias Clasificadas del Ministerio de Defensa tiene por finalidad asegurar el correcto manejo de la información clasificada, en cualquier formato, ámbito o situación en que se encuentre y, en concreto, el registro, manejo, distribución, control y archivo de los documentos clasificados de acuerdo con la normativa en vigor.

Decimocuarta. *Estructura del Servicio de Protección de Materias Clasificada*s.

El Servicio de Protección de Materias Clasificadas tendrá la siguiente estructura funcional:

a) En el nivel corporativo se establece el Servicio Central de Protección de Materias Clasificadas del Ministerio de Defensa, que estará bajo la autoridad del Director del CESTIC.

b) En cada ámbito del nivel específico habrá, al menos, un Servicio General de Protección de Materias Clasificadas, con dependencia funcional del Servicio Central de Protección de Materias Clasificadas del Ministerio de Defensa, que estará bajo la autoridad del Jefe de Seguridad de la Información del ámbito correspondiente.

CVE: BOD-2016-171-21250

c) En las unidades, centros y organismos cuando sea necesario el uso y custodia de documentos clasificados, se establecerá un Servicio Local de Protección de Materias Clasificadas, con dependencia funcional del Servicio General de Protección de Materias Clasificadas del ámbito correspondiente, que estarán bajo la autoridad del Jefe de la unidad a la que da servicio.

CAPITULO III

Gobierno de la seguridad de la información del Ministerio de Defensa

Decimoquinta. *Gobierno de la seguridad de la información del Ministerio de Defensa*.

1. El gobierno de la seguridad de la información del Ministerio de Defensa, constituye el marco de referencia dentro del cual se desarrollará el seguimiento, coordinación y control de la Política de Seguridad de la Información del Departamento y su normativa de aplicación.

2. Este gobierno se articula en:

a) El Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa (CDSIDEF), establecido en la Orden Ministerial 76/2006, de 19 de mayo, que será el órgano colegiado responsable de la coordinación y seguimiento de la Política de Seguridad de la Información a nivel departamental.

b) La Comisión Ejecutiva de la Seguridad de la Información del Ministerio de Defensa (CESIDEF), órgano para la coordinación, el seguimiento y control del Plan de Actuación que complementará el desarrollo normativo de la Política de Seguridad de la Información, llevará a cabo los cometidos e indicaciones emanadas del DSIDEF y la coordinación entre los niveles y ámbitos de la estructura funcional.

c) Los Comités de la Seguridad de la Información del Ministerio de Defensa, como órganos para el seguimiento y control de los Planes de Acción de las diferentes áreas que se deriven del Plan de Actuación para la Seguridad de la Información. Se establece un Comité por cada área de seguridad de la información:

1º. Comité de SEGINFOPER.
2º. Comité de SEGINFODOC.
3º. Comité de SEGINFOINS.
4º. Comité de SEGINFOEMP.
5º. Comité de SEGINFOSIT.

3. El CESTIC desempeñará las funciones de asistencia y apoyo a todos estos órganos de gobierno.

Decimosexta. *Composición del Consejo de Dirección de la Seguridad de la Información.*

La composición del Consejo de Dirección de la Seguridad de la Información será la establecida en el apartado cuarto de la Orden Ministerial 76/2006, de 19 de mayo, actualizada atendiendo a las correspondientes modificaciones en la estructura orgánica que se hayan producido desde la aprobación de dicha orden ministerial.

Decimoséptima. *Cometidos del Consejo de Dirección de la Seguridad de la Información.*

1. El Consejo de Dirección de la Seguridad de la Información es el órgano responsable de la coordinación y seguimiento de la Política de Seguridad de la Información del Ministerio, y para ello desarrollará las siguientes funciones:

a) Coordinar la implantación de la Política de Seguridad de la Información del Ministerio de Defensa, velando por su coherencia con las disposiciones de dicha política.

b) Seguir el desarrollo de la Política de Seguridad de la Información a través de los informes anuales, así como de los procedentes de la CESIDEF, para mantener su coherencia y aprobar, en su caso, las medidas para corregir las deficiencias identificadas.

CVE: BOD-2016-171-21251

c) Coordinar, realizar el seguimiento y controlar la elaboración y cumplimiento de la normativa de 2º nivel de aplicación de la Política de Seguridad de la Información, así como de los planes, programas y procedimientos elaborados por los Responsables de las Áreas de Seguridad de la Información, y de aplicación a todo el Ministerio.

d) Coordinar la posición única del Ministerio de Defensa en los foros internacionales y en su relación con otros Departamentos y Organizaciones de las Administraciones Públicas.

e) Dar directrices a la CESIDEF sobre cualquier asunto de su competencia.

2. El CDSIDEF se reunirá con carácter general en sesión ordinaria al menos una vez al año mediante convocatoria de su Presidente, o bien en convocatoria extraordinaria a iniciativa del propio Presidente o cuando lo soliciten, al menos, la mitad de sus miembros.

Decimoctava. *Composición de la Comisión Ejecutiva de Seguridad de la Información*.

1. La Comisión Ejecutiva de Seguridad de la Información del Ministerio de Defensa, estará compuesta por los siguientes miembros:

a) Presidente: El Director del CESTIC.

b) Vocales: Los Jefes de Seguridad de la Información (JSI) de los ámbitos específicos:

1º. JSI del EMAD.
2º. JSI de la SEDEF.
3º. JSI de la SUBDEF.
4º. JSI del ET.
5º. JSI de la AR.
6º. JSI del EA.
7º. JSI de la SEGENPOL.

Serán igualmente vocales de esta comisión los cinco Responsables de cada una de las Áreas de Seguridad de la Información definidos en la norma sexta. c), o personal específicamente designado por estos.

c) Secretario: Un oficial de empleo Coronel, Capitán de Navío o funcionario de nivel 29 de la estructura del CESTIC, designado por el Presidente de la Comisión Ejecutiva.

2. Con carácter general la Comisión Ejecutiva se reunirá en sesión ordinaria dos veces al año mediante convocatoria de su Presidente, o bien en convocatoria extraordinaria a iniciativa del propio Presidente o cuando lo soliciten, al menos, la mitad de sus miembros.

Decimonovena. *Cometidos de la Comisión Ejecutiva de la Seguridad de la Información.*

La Comisión Ejecutiva de la Seguridad de la Información del Ministerio de Defensa en virtud de las atribuciones que establece la norma decimoquinta. 2.b) tendrá los siguientes cometidos:

a) Llevar a cabo el seguimiento del Plan de Actuación para la Seguridad de la Información y su correspondiente normativa en materia de seguridad de la información en las personas, en los documentos, en las instalaciones, en los sistemas de información y telecomunicaciones y en poder de las empresas, así como atender y cumplimentar las directrices que emanen del DSIDEF.

b) Coordinar la ejecución del Plan de Actuación para la Seguridad de la Información que desarrollará la Política, incluidos los respectivos Planes de Acción de las diferentes áreas.

c) Definir los Planes de Acción del nivel corporativo para desarrollar el Plan de Actuación para la Seguridad de la Información, que complementarán el desarrollo normativo de tercer nivel establecido en la Política de Seguridad de la Información del Ministerio de Defensa. Dar directrices a los Comités de Seguridad de la Información sobre la ejecución de los citados Planes.

d) Revisar los informes emitidos por los Comités de Seguridad de la Información y en su caso proponer modificaciones sobre los Planes de Acción de las áreas para corregir las deficiencias detectadas.

CVE: BOD-2016-171-21252

e) Informar al DSIDEF del resultado de sus reuniones así como del estado de ejecución del Plan de Actuación y de los respectivos Planes de Acción.

f) Establecer los Comités que se consideren necesarios para el seguimiento de aspectos de seguridad de la información concretos que afecten a varias áreas de Seguridad, para proponer al CDSIDEF soluciones a los mismos.

g) Dar directrices a los Comités de Seguridad de la Información sobre cualquier asunto de su competencia.

h) Supervisar los resultados de los informes anuales. Proponer al CDSIDEF las métricas e indicadores más adecuados para valorar el estado de seguridad de la información. Informar al CDSIDEF anualmente del estado de avance del Plan de Actuación para la Seguridad de la Información en el que se identifiquen riesgos y deficiencias.

i) Revisar las normativas de tercer nivel de carácter corporativo para su aprobación por el Director del CESTIC.

j) Asegurar la necesaria coordinación entre todas las áreas y ámbitos de la seguridad de la información.

Vigésima. *Composición de los Comités de Seguridad de la Información.*

1. Cada Comité de Seguridad de la Información de un área determinada, estará compuesto por los siguientes miembros:

a) Presidente: El Responsable del Área de Seguridad de la Información correspondiente.

b) Vocales: Los Jefes de las Áreas de Seguridad de la Información (JAS) de los ámbitos del nivel específico.

1.º JAS del EMAD.
2.º JAS de la SEDEF.
3.º JAS de la SUBDEF.
4.º JAS del ET.
5.º JAS de la AR.
6.º JAS del EA.
7.º JAS de la SEGENPOL.

c) Secretario: Un oficial de empleo Coronel, Capitán de Navío o funcionario de nivel 29, designado por el Presidente del Comité.

2. Los Presidentes de los diferentes Comités contarán con la asistencia y apoyo del CESTIC para el desarrollo de sus cometidos.

Vigesimoprimera. *Cometidos de los Comités de Seguridad de la Información.*

Los Comités de Seguridad de la Información son los órganos responsables del seguimiento y control de los Planes de Acción en las diferentes áreas de seguridad de la información. Tendrán los siguientes cometidos:

a) Efectuar el seguimiento y control de los Planes de Acción de las Áreas de Seguridad de la Información que emanen del Plan de Actuación para la Seguridad de la Información, conforme a las directrices de los responsables de las áreas de seguridad de la información.

b) Efectuar el seguimiento y control de los Planes de Acción que procedan de la Comisión Ejecutiva conforme a sus criterios y directrices.

c) Supervisar la ejecución de dichos Planes comprobando el cumplimiento de los objetivos marcados y proponer, en su caso, medidas correctoras.

d) Informar a la Comisión Ejecutiva de los resultados de las actividades, los riesgos y la problemática, así como de las inversiones y los gastos derivados de la ejecución del respectivo Plan de Acción.

CVE: BOD-2016-171-21253

ANEXO

Plan de Actuación para la Seguridad de la Información y su desarrollo

El desarrollo normativo de la Política de Seguridad de la Información se complementará, entre otras medidas, mediante la elaboración y ejecución del Plan de Actuación para la Seguridad de la Información con un alcance de medio plazo y de los correspondientes Planes de Acción a corto plazo, orientados en cada una de las áreas de seguridad de la información, alineados con los recursos financieros y materiales, derivados del proceso de Planeamiento de la Defensa.

El Plan de Actuación para la Seguridad de la Información contemplará, al menos, los siguientes aspectos:

a) Introducción con un resumen ejecutivo de la Política de la que deriva.
b) Ámbito, alcance y líneas generales.
c) Concreción de las relaciones entre los órganos de planeamiento y los órganos de ejecución en el ámbito de competencias del Departamento.
d) Criterios generales para la formación del personal.
e) Criterios generales para la aplicación de medidas de seguridad de la información.
f) Necesidades de recursos humanos, materiales y financieros para el desarrollo del Plan de Actuación.
g) Directrices para la transición desde la situación actual a la deseada.
h) Directrices para los Planes de Acción, opciones y escenarios, métricas, riesgos asociados y su gestión. Entre las directrices a contemplar se establecerán los responsables de la elaboración y aprobación de los Planes de Acción, teniendo en cuenta lo establecido en las presentes normas.
i) Planificación temporal de las tareas y acciones previstas.

Los Planes de Acción en las diferentes áreas de seguridad de la información que se deriven de la citada Política de Seguridad de la Información, desarrollarán específicamente y en detalle para el área de seguridad de la información concreta los diferentes aspectos del Plan de Actuación para la Seguridad de la Información, desde un punto de vista técnico, funcional u operativo. Incluirán todos los factores relacionados con las medidas de seguridad de la información y los recursos y organización necesarios para su desarrollo. Cada Plan de Acción establecerá las medidas de seguridad de la información necesarias en su área de seguridad de la información.

CVE: BOD-2016-171-21254