I. — DISPOSICIONES GENERALES

ORGANIZACIÓN

Instrucción 96/2011, de 16 de diciembre, del Secretario de Estado de Defensa por la que se crea el Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa.

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, designa en su apartado primero como Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF) al Secretario de Estado de Defensa, y se le encomienda en este mismo apartado las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información en el ámbito del Ministerio de Defensa.

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, se designa en la disposición adicional única de dicha instrucción al Director General de Infraestructura (DIGENIN) como responsable de las áreas de seguridad de la información en las personas, en los documentos, en las instalaciones y en los sistemas de información y telecomunicaciones, siendo en el ejercicio de los citados cometidos, el interlocutor a nivel corporativo, del Ministerio de Defensa con el Centro Nacional de Inteligencia y organismos externos al Departamento, con facultad de representar al Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF) en el ámbito de sus competencias.

El artículo 6 del Real Decreto 1287/2010, de 15 de octubre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, establece que la DIGENIN, a través de su Subdirección General de Tecnologías de la Información y Comunicaciones, desarrolla las funciones de dirección y gestión de las infraestructuras, los servicios y ciclo de vida de los sistemas de información y telecomunicaciones de ámbito corporativo para Propósito General y, define las políticas y estrategias corporativas en el ámbito de las tecnologías de la información, comunicaciones y seguridad de la información del Ministerio de Defensa, así como la planificación y coordinación de las actuaciones en estas materias.

El objetivo de la Política de Seguridad de la Información del Ministerio es alcanzar la protección adecuada, proporcionada y razonable de la información y para ello es necesario hacer frente a las potenciales amenazas a las que se enfrentan los sistemas de información del Departamento. Para la consecución de dicho objetivo deben emprenderse labores de monitorización continua de los sistemas de información y telecomunicaciones que permitan detectar de forma temprana los posibles incidentes de seguridad y emprender las acciones reactivas pertinentes, que en caso de materializarse, minimicen su impacto y conlleven a su resolución.

Distintas organizaciones, tanto nacionales como internacionales, con el objetivo de mejorar sus capacidades en la protección de los sistemas de información y telecomunicaciones de importancia crítica frente a ciberataques, han visto la necesidad de disponer de una capacidad operativa completa de respuesta ante incidentes de seguridad y han desarrollado o están desarrollando para ello en sus respectivos ámbitos el concepto de ciberdefensa.

Por todo ello, se hace necesario, constituir el Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa (COSDEF), estableciendo su estructura y cometidos. Este centro prestará los servicios necesarios de seguridad de la información y ciberdefensa para los Sistemas de Información y Telecomunicaciones de Propósito General con los que permitir en el nivel corporativo, emprender acciones encaminadas a reducir el riesgo de actividades que vayan en contra de la seguridad de la información en dichos sistemas y mitigar el impacto de los ataques cuando estos se produzcan. De esta forma

CVE: BOD-2011-251-33507

podrá conseguirse una capacidad operativa completa de respuesta ante incidentes de seguridad, actuando de forma proactiva, rápida y coordinada con todos los agentes del Departamento con competencias en la materia.

La disposición final primera de la Orden Ministerial 76/2006, de 18 de mayo, faculta al Secretario de Estado de Defensa facultades a dictar las disposiciones oportunas, en el ámbito de sus competencias, para el desarrollo y ejecución de dicha orden ministerial.

Esta instrucción cuenta con el informe preceptivo de la Comisión Ministerial de Administración Electrónica del Ministerio de Defensa conforme al artículo 3.e) de la Orden DEF/1159/2010, de 3 de mayo, por la que se regula dicha comisión.

En su virtud,

DISPONGO:

Primero. *Creación.*

Se crea el Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa (COSDEF), con la misión de gestionar las actividades de operación de carácter proactivo, reactivo y de detección, relacionadas con la seguridad de la información y ciberdefensa en los sistemas de información y telecomunicaciones corporativos.

Segundo. *Alcance.*

El COSDEF prestará sus servicios a nivel corporativo en los Sistemas de Información y Telecomunicaciones de Propósito General del Ministerio de Defensa.

Tercero. *Definiciones.*

A los efectos de la presente Instrucción, se considera:

- Actividades de detección: Conjunto de operaciones conducentes a detectar posibles incidentes de seguridad de forma temprana, efectuando para ello labores de monitorización de los distintos sistemas y llevando a cabo la explotación de herramientas de detección y prevención de intrusiones.
- Actividades de gestión: Conjunto de acciones encaminadas a la operación propia de los sistemas de seguridad de la información y a la obtención y presentación de información sobre el estado de seguridad de los Sistemas de Información y Telecomunicaciones (SIT).
- Actividades proactivas: Conjunto de operaciones dirigidas al análisis de las amenazas que pueden materializarse en los SIT, a la detección y análisis de vulnerabilidades en dichos sistemas, así como a promover la implantación de medidas de seguridad de carácter preventivo.
- Actividades reactivas: Conjunto de operaciones orientadas a evaluar y resolver incidentes de seguridad que pudieran causar un impacto en la organización así como a realizar a posteriori, análisis de tipo forense para averiguar qué ha ocurrido al objeto de proponer acciones correctivas para evitar la repetición de incidentes similares.
- Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales.
- Ciberdefensa: Conjunto organizado de recursos, actividades y procedimientos orientados a preservar la seguridad de los sistemas de información y telecomunicaciones propios, así como la información que manejan, con el objeto de garantizar el acceso al ciberespacio y facilitar el uso eficiente de los recursos.
- Incidente de Seguridad: cualquier situación o eventualidad en la que pueda verse amenazada la información, y pueda en consecuencia dar lugar a una pérdida de confidencialidad, integridad o disponibilidad de ésta.
- Entorno de propósito general: Entorno de los SIT del Ministerio que no son específicos de Mando y Control Militar.
- Organización CIS: Conjunto de personas y organismos del Ministerio de Defensa que tiene asignados cometidos relativos a la gestión, operación y manejo de Sistemas de

CVE: BOD-2011-251-33508

Información y Telecomunicaciones del Ministerio de Defensa. Se hace referencia a ellos por su acrónimo en Inglés (CIS- Communications and Information Systems).

- Vulnerabilidad: Debilidad, atributo o pérdida de control que permitiría o facilitaría la materialización de una amenaza.

Cuarto. *Cometidos*.

El COSDEF, en el ámbito de sus actividades de apoyo técnico al Responsable de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones, asumirá los siguientes cometidos y cualquier otro que en las áreas de su competencia le sea asignado:

a) Proactivos:

1.º Analizar las amenazas conocidas, valorar su potencial impacto en caso de su materialización y, cuando corresponda, informar al responsable del área de seguridad de la información en los Sistemas de Información y Telecomunicaciones.

2.º Identificar y analizar las posibles vulnerabilidades de los Sistemas de Información y Telecomunicaciones, clasificarlas según su criticidad e informar a los responsables de dichos sistemas para que adopten las medidas correctivas pertinentes.

3.º Realizar recomendaciones y promover la implantación de medidas de seguridad de carácter preventivo.

b) De detección:

1.º Monitorizar los Sistemas de Información y Telecomunicaciones buscando signos de intrusiones y otras actividades anómalas, pudiendo integrar los elementos de control del resto de áreas de seguridad de la información con el objetivo de conseguir una visión integral de la seguridad de la información.

2.º Gestionar e inspeccionar los registros de actividad de los Sistemas de Información y Telecomunicaciones, para garantizar el cumplimiento de los requisitos de seguridad correspondientes a la normativa de aplicación vigente.

c) Reactivos:

1.º Gestionar la capacidad corporativa de respuesta a incidentes de seguridad de la información, así como determinar y dirigir las actuaciones necesarias a adoptar en los Sistemas de Información y Telecomunicaciones, coordinando y colaborando en la ejecución de este proceso con los responsables implicados, así como con cualquier organismo del Ministerio que se considere que deba participar o ser informado.

2.º Llevar a cabo la investigación y análisis forense consecuente a resultas de los incidentes de seguridad identificados.

3.º Proponer acciones correctivas para evitar la repetición de incidentes de seguridad.

d) De gestión:

1.º Informar del estado de las actividades del COSDEF.

2.º Ejecutar acciones de formación, concienciación y sensibilización en materia de seguridad de la información y ciberdefensa.

3.º Promover ejercicios de ciberdefensa en el Ministerio de Defensa y participar en lo posible en los ejercicios que se desarrollen en otros foros tanto nacionales como internacionales.

4.º Explotar y administrar los Sistemas de Información y Telecomunicaciones del COSDEF.

5.º Contribuir a la mejora del nivel de seguridad de los Sistemas de Información y Telecomunicaciones de todo el Ministerio de Defensa, colaborando con otros organismos o departamentos del MINISDEF que lleven a cabo tareas de seguridad de la información.

6.º Colaborar con otros centros de operaciones de seguridad con capacidad de respuesta ante incidentes del Ministerio de Defensa, con objeto de aprovechar y compar-

CVE: BOD-2011-251-33509

tir conocimientos y experiencias adquiridas, estableciendo una sinergia positiva entre las partes.

Quinto. *Dependencia orgánica y relaciones funcionales.*

1. El Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa (COSDEF) se encuadra en la Subdirección General de Tecnologías de la Información y Comunicaciones.

2. Para llevar a cabo sus cometidos, el COSDEF podrá establecer relaciones funcionales con cualquier integrante de la organización CIS del Departamento, en el ámbito de las actividades del Centro.

3. El COSDEF podrá establecer relaciones directas, según se determine en cada caso, con otros centros operativos de seguridad del Ministerio de Defensa.

Sexto. *Estructura organizativa.*

1. El COSDEF tendrá la siguiente estructura:

a) Célula de Prevención que desarrollará los cometidos señalados en el apartado cuarto.a).

b) Célula de Detección y Operación que desarrollará los cometidos señalados en el apartado cuarto.b).

c) Célula de Reacción que desarrollará los cometidos señalados en el apartado cuarto.c).

d) Célula de Soporte que desarrollará los cometidos señalados en el apartado cuarto.d).

2. El personal que preste sus servicios en el COSDEF así como, el personal que realice actividades temporales en virtud de un contrato con el Ministerio de Defensa, deberá disponer de la habilitación personal de seguridad (HPS) correspondiente.

Disposición derogatoria única.

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

Disposición final. *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 de 2011.—El Secretario de Estado de Defensa, Constantino Méndez Martínez.

CVE: BOD-2011-251-33510