V. — OTRAS DISPOSICIONES

NORMAS

Resolución 300/05090/18

Cód. Informático: 2018007380.

Resolución del Secretario de Estado de Defensa, por la que se aprueba el Plan de Actuación para la 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 Orden Ministerial 76/2006, de 19 de mayo, establece como objeto de la citada política *"alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa"*.

El apartado octavo, de esta política establece que se desarrollará el correspondiente cuerpo normativo sobre Seguridad de la Información (SEGINFO), enmarcando cada conjunto de normas en distintos niveles por amplitud del aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

En el marco de este proceso de desarrollo normativo, por Instrucción 53/2016, de 24 de agosto, del Secretario de Estado de Defensa, se aprobaron las *"Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa".* La norma primera. c) establece, como una de las finalidades, la de *"Regular el Plan de Actuación para la Seguridad de la Información y su desarrollo mediante Planes de Acción",* atribuyéndose en la norma cuarta.1, al Secretario de Estado de Defensa, la competencia para aprobar el citado plan.

El Plan de Actuación para la Seguridad de la Información facilitará, con el contenido que se establece en el anexo a las normas aprobadas por la Instrucción 53/2016, de 24 de agosto, facilita el desarrollo de la Política de SEGINFO.

Por Orden DEF/2639/2015, de 3 de diciembre, se estableció la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (Política CIS/TIC). Uno de los principios de esta Política consiste en la Seguridad en los sistemas y servicios de manera que la protección de la información no afecte a su tratamiento o transmisión. Por su parte, uno de sus ejes estratégicos de esta Política es el relativo a la consolidación de 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 SEGINFO del Ministerio de Defensa.

Es imprescindible el alineamiento entre el desarrollo de la Política CIS/TIC, materializado en el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS) y el de la Política de SEGINFO en lo relativo a los CIS/TIC. El desarrollo de esta última, en primer lugar en el Plan de Actuación para la SEGINFO, debe ser coherente por tanto con los principios finalidad, ejes estratégicos y directrices de la Política CIS/TIC.

De igual manera, el Plan de Actuación para la SEGINFO debe alinearse con la Política en materia de Seguridad de la Información de la Administración General del Estado y de las Organizaciones Internacionales de las que España forma parte.

Por cuanto antecede, en el ejercicio de las competencias que me atribuye la norma cuarta.1 de las Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa, aprobadas por Instrucción 53/2016, de 24 de agosto, del Secretario de Estado de Defensa,

CVE: BOD-2018-070-8478

DISPONGO:

Primero. *Aprobación del Plan de Actuación para la Seguridad de la Información del Ministerio de Defensa.*

Se aprueba el Plan de Acción para la Seguridad de la Información del Ministerio de Defensa (PA SEGINFO), cuyo texto se inserta como Anexo a esta Resolución.

Segundo. *Facultades de coordinación.*

Se faculta al Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones para dictar, en el ámbito de sus competencias, las disposiciones oportunas para la aplicación de esta Resolución.

Tercero. *Efectos.*

La presente Resolución surtirá efectos a partir del día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, a 24 de noviembre de 2017. El Secretario de Estado de Defensa, Agustín Conde Bajén.

CVE: BOD-2018-070-8479

ANEXO

PLAN DE ACTUACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN
DEL MINISTERIO DE DEFENSA

(PA SEGINFO)

RESUMEN EJECUTIVO

El Plan de Actuación para la Seguridad de la Información del Ministerio de Defensa (PA SEGINFO) es un instrumento de planeamiento para el desarrollo de la Política de Seguridad de la Información del MDEF (Política SEGINFO), aprobada por la Orden Ministerial 76/2006, de 19 de mayo.

El PA SEGINFO establece la hoja de ruta a seguir en el proceso de identificación y desarrollo de las medidas de SEGINFO y los Planes de Acción para lograr lo establecido en la Política SEGINFO y en la Instrucción 53/2016, de 24 de agosto, por la que se aprueban las Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa.

El PA SEGINFO constituye la guía para la identificación y desarrollo de las medidas de SEGINFO, y de los distintos procesos y estructuras necesarios para su adecuado funcionamiento. Así mismo, es un instrumento de coordinación con el Eje Estratégico 5 de la Secretaría de Estado de Defensa, con el Plan de Acción del MDEF para la Transformación Digital (partes 1 y 2), según lo establecido en la Orden DEF/2071/2015, de 5 de octubre, y con el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS) que desarrolla la Política CIS/TIC, establecida en la Orden DEF/2639/2015, de 3 de diciembre.

Conforme a lo establecido en el Anexo de la citada Instrucción 53/2016, el PA SEGINFO contempla:

• Objetivos Estratégicos (OE). Los OE tienen como finalidad el desarrollo de la Política SEGINFO y son la referencia de este PA SEGINFO y de los diferentes Planes de Acción.

• Líneas de Acción. A su vez, para cada Objetivo Estratégico se identifican Líneas de Acción para su consecución. Estas Líneas de Acción constituyen, junto a los principios básicos de la Política SEGINFO y de este PA SEGINFO, la referencia principal para el desarrollo de los diferentes Planes de Acción.

• Apéndices:

– Apéndice I. Diagrama de Gantt con la secuencia prevista a alto nivel para alcanzar los Objetivos Estratégicos y Líneas de Acción a lo largo del periodo 2018-2023.

– Apéndice II. Criterios Generales para la aplicación de medidas de seguridad de la información y para la formación de personal.

– Apéndice III. Directrices para la transición desde la situación actual a la situación deseada.

– Apéndice IV. Directrices sobre la estructura general de los Planes de Acción y directrices que guiarán el control y seguimiento de los mismos.

– Apéndice V. Necesidades de recursos humanos, que se estiman necesarios para la consecución de los Objetivos del PA SEGINFO.

– Apéndice VI. Necesidades de recursos financieros, para afrontar las inversiones y gastos requeridos que permitan la consecución de los Objetivos del PA SEGINFO.

– Apéndice VII. Normativa de Aplicación.

CVE: BOD-2018-070-8480

– Apéndice VIII. Abreviaturas y Acrónimos.

Conforme a lo establecido en la Instrucción 53/2016, los citados Planes de Acción desarrollarán los objetivos estratégicos recogidos en el PA SEGINFO identificando, entre otros aspectos, las medidas necesarias para desarrollar 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.

Figura 1. Contexto General del PA SEGINFO.

1. OBJETO

Según establece en su disposición cuarta la Instrucción 53/2016, por la que se aprueban las Normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa (Política SEGINFO), este Plan de Actuación tiene por objeto facilitar el desarrollo de la Política de SEGINFO, aprobada por la Orden Ministerial 76/2006, y complementar el desarrollo normativo establecido en el apartado octavo de dicha Política.

Con este fin, el propósito de este documento es proporcionar un plan de actuación que se desarrollará, conforme a lo establecido en las citadas Política de SEGINFO e Instrucción 53/2016, con un alcance de medio plazo, a través de los correspondientes planes de acción a corto plazo, orientados a materias concretas de la SEGINFO, alineados con los recursos financieros y materiales, derivados del proceso de Planeamiento de la Defensa. Los citados planes de acción desarrollarán los objetivos estratégicos recogidos en el PA SEGINFO identificando, entre otros aspectos, las medidas necesarias para desarrollar 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, conforme a lo establecido en la Instrucción 53/2016.

CVE: BOD-2018-070-8481

2. ALCANCE

Este Plan de Actuación recoge todas las medidas para el desarrollo de la Política de SEGINFO del MDEF y tendrá un horizonte temporal de medio plazo (6 años), desde enero de 2018 a diciembre de 2023. En concreto, abordará la definición de todas aquellas normas, procedimientos y esquemas de organización necesarios para la aplicación de la Política de SEGINFO y la consecución de la protección de la información en el MDEF.

Se desarrollará a través de un Plan de Acción General de SEGINFO y de los correspondientes Planes de Acción, de cada una de las Áreas de Seguridad de la Información definidas en la Orden Ministerial 76/2006. Estos Planes de Acción tendrán un alcance a corto plazo (entre uno y tres años) y estarán alineados con los recursos financieros y materiales, derivados del proceso de Planeamiento de la Defensa, regulado en la Orden Ministerial 60/2015, de 3 de diciembre.

3. ÁMBITO DE APLICACIÓN

Este Plan de Actuación será de aplicación a todo el Ministerio de Defensa y sus Organismos Públicos.

4. CALENDARIO

Para su desarrollo se plantean dos fases sucesivas:

- Fase I: 2018 - 2020.
- Fase II: 2021 - 2023.

En el Apéndice I se describe en detalle la previsión de plazos para la ejecución de las líneas de acción previstas en este PA SEGINFO, en cada una de las fases.

Este calendario permite el alineamiento con el Ciclo de Planeamiento de la Defensa 2017-2024 (cuya fase de definición incluye el periodo 2017-2018 y su fase de ejecución el 2019-2024, atendiendo a lo regulado en la Orden Ministerial 60/2015, de 3 de diciembre, por la que se regula el proceso de Planeamiento de la Defensa). En 2023 se iniciaría la fase de definición del nuevo Ciclo de Planeamiento de la Defensa 2023-2030.

Así mismo permite el alineamiento con el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS) que desarrolla la Política CIS/TIC y constituye la referencia para el desarrollo de medidas de Seguridad de la Información en el ámbito tecnológico.

5. ANTECEDENTES Y CONTEXTO ACTUAL

La Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información (SEGINFO) del Ministerio de Defensa, establece que es objeto de la misma alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa. En su apartado octavo, se establece que se desarrollará el correspondiente cuerpo normativo sobre SEGINFO, enmarcando cada conjunto de normas en distintos niveles por amplitud del aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

En el marco de este proceso de desarrollo normativo se aprobó la 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. Dichas normas tienen por finalidad establecer la estructura funcional de la SEGINFO del MDEF, definir la estructura de gobierno de la SEGINFO del Departamento y regular el Plan de Actuación para la Seguridad de la Información y su desarrollo mediante Planes de Acción.

El Plan de Actuación para la Seguridad de la Información facilitará el desarrollo de la Política de SEGINFO, complementado el desarrollo normativo establecido en el citado apartado octavo de la Política de SEGINFO, siguiendo lo dispuesto en el Anexo de la Instrucción 53/2016, de 24 de agosto en cuanto a su objeto y estructura mínima.

CVE: BOD-2018-070-8482

En concreto, en dicho Anexo se especifica que el PA SEGINFO, con un alcance a medio plazo, deberá contemplar entre otros aspectos, la concreción de las relaciones entre los órganos de planeamiento y los órganos de ejecución en el ámbito de competencias del Departamento, las directrices que deben guiar la elaboración de los planes de acción, las directrices para la transición desde la situación actual a la deseada y los criterios generales para la formación del personal en materia SEGINFO y para la aplicación de medidas en este ámbito.

La citada Instrucción 53/2016, establece en su capítulo III que tanto el PA SEGINFO como los Planes de Acción que lo desarrollan estarán bajo el seguimiento y el control de la estructura de gobierno de la SEGINFO del MDEF recogida en la misma,

La Orden DEF/2639/2015, de 3 de diciembre, establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (Política CIS/TIC). Uno de los principios de dicha Política CIS/TIC es la seguridad en los sistemas y servicios CIS/TIC de manera que la protección de la información no afecte a su tratamiento o transmisión, y 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 SEGINFO del Ministerio de Defensa.

Por la Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, se aprobó la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC). En la citada arquitectura se describen a alto nivel las Capacidades y los Servicios CIS/TIC necesarios para cumplir la Finalidad y los Ejes Estratégicos de la Política CIS/TIC, así como los Requisitos Principales y Operativos de las citadas Capacidades CIS/TIC.

Por todo lo anterior, es imprescindible el alineamiento del Plan de Actuación para la SEGINFO que desarrolla la Política de SEGINFO, con el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS), que desarrolla la Política CIS/TIC. En consecuencia, el PA SEGINFO debe ser coherente con los principios finalidad, ejes estratégicos y directrices de la Política CIS/TIC.

Así mismo, debe tomar en consideración lo establecido en la AG CIS/TIC en relación con las normas y procedimientos de Seguridad de la Información que deben cumplirse. Dentro de los procesos funcionales y operativos (incluidos en la Vista de Capacidades Operativas), se incluyen los procesos de Seguridad de la Información, como aquél conjunto de procesos que se deben implantar y ejecutar para proporcionar un nivel de seguridad aceptable de la información manejada por las personas, en la documentación, instalaciones, empresas y por los sistemas de información y telecomunicaciones, permitiendo crear un entorno seguro de los CIS/TIC que cumpla con los requisitos de seguridad para el manejo de información. Por ello, es imprescindible que el PA SEGINFO esté alineado con la provisión de las Capacidades de Seguridad CIS/TIC del Ministerio de Defensa, cuya taxonomía se incluye en el Apéndice VII de la AG CIS/TIC.

Por último, se han aprobado una serie de regulaciones e iniciativas en materia de Seguridad de la Información a nivel de la Administración General del Estado (fundamentalmente el Esquema Nacional de Seguridad, regulado por Real Decreto 3/2010, de 8 de enero y actualizado por el Real Decreto 951/2015, de 23 de octubre, la Estrategia de Ciberseguridad Nacional de 2013, la normativa relativa a la Protección de Datos de Carácter Personal y las políticas, procedimientos, normas y guías desarrolladas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) y de las Organizaciones Internacionales de las que España forma parte, con las cuales también debe alinearse el PA SEGINFO.

6. OBJETIVOS ESTRATÉGICOS

Los Objetivos Estratégicos del PA SEGINFO (OE) tienen como finalidad el desarrollo de la Política SEGINFO y son la referencia de este PA SEGINFO y de los diferentes Planes de Acción.

CVE: BOD-2018-070-8483

El PA SEGINFO desarrolla los citados Objetivos Estratégicos en Líneas de Acción, y éstas a su vez se deben desarrollar en Actuaciones en los correspondientes Planes de Acción.

OE 1. COMPLETAR EL DESARROLLO DE LA NORMATIVA DE SEGURIDAD DE SEGUNDO Y TERCER NIVEL Y ESTABLECER UN PROCESO DE REVISIÓN CONTINUA.

El marco normativo del MDEF plantea un escenario de cambio y transformación, que establece la necesidad de adecuar la normativa existente a las nuevas circunstancias, condicionantes y necesidades del MDEF en este ámbito, y elaborar nueva normativa en materia de seguridad de la información, estableciendo así mismo un proceso de revisión continua.

Este objetivo tiene como finalidad asegurar tanto la consistencia con la normativa interna como externa al Departamento, así como la identificación de aquellos problemas u oportunidades de mejora, por parte de los responsables de cada área de seguridad.

Líneas de Acción Asociadas:

LA 1.1. Revisar y actualizar la OM 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa.
LA 1.2. Actualizar y completar el desarrollo normativo de segundo nivel de la Política de SEGINFO del MDEF.
LA 1.3. Actualizar y completar el desarrollo normativo de tercer nivel de la Política de SEGINFO del MDEF.
LA 1.4. Definir e implantar un procedimiento de revisión periódica de la normativa de desarrollo de la Política de SEGINFO.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

El Plan de Acción de cada área de SEGINFO deberá desarrollar este objetivo, incluyendo las medidas de seguridad necesarias para su cumplimiento.

OE 2. INCREMENTAR EL GRADO DE CUMPLIMIENTO Y ADECUACIÓN A LA LEGISLACIÓN VIGENTE SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

El Ministerio de Defensa debe cumplir con la legislación vigente en materia de protección de datos (la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD), así como, con la Política de Seguridad de la Información del Ministerio de Defensa, alineándose las directrices de Seguridad de la Información al nuevo Reglamento General de Protección de Datos (RGPD) de la UE, aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La Instrucción 16/2017, de 31 de marzo, del Secretario de Estado de Defensa, por la que se aprueban las normas de seguridad de la información que contenga datos de carácter personal en el Ministerio de Defensa, define los principios generales de Seguridad de la Información en materia de protección de datos de carácter personal a implantar en el Departamento, además de describir la estructura funcional del mismo para esta materia.

Este objetivo tiene como propósito adaptar la estructura funcional y los procesos a las nuevas directrices establecidas tanto por el Reglamento Europeo (que entrará en vigor el 25 de mayo del 2018), como por la citada Instrucción 16/2017.

Líneas de Acción Asociadas:

LA 2.1. Inventariar todos los sistemas de tratamiento de datos críticos para facilitar el control de aquellos sistemas con datos de carácter personal de nivel alto en los que, en un momento determinado, pudiera existir un posible riesgo de fuga de información.

CVE: BOD-2018-070-8484

LA 2.2. Elaborar análisis de riesgos alineados con el Esquema Nacional de Seguridad (ENS).

El análisis de riesgos es una de las novedades del RGPD, y siguiendo las pautas marcadas por el ENS, se pretende detectar las posibles amenazas y prever los daños y consecuencias que éstas puedan producir.

LA 2.3. Desarrollar una metodología de identificación y comunicación con la Agencia Española de Protección de Datos (AEPD) sobre las brechas de seguridad, realizando gestión de incidencias y aprovechando los canales actuales de dicha gestión.

LA 2.4. Crear y consolidar la estructura funcional para la protección de datos de carácter personal en el Ministerio de Defensa.

LA 2.5. Adecuar las estructuras y procedimientos en materia de protección de datos de carácter personal al Reglamento General de Protección de Datos (RGPD) de la UE.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

Este objetivo será desarrollado por el CESTIC, como Oficina Central de Protección de Datos de Carácter Personal del MDEF, que elaborará las medidas necesarias para cumplir con los objetivos.

OE 3. INCREMENTAR EL GRADO DE CUMPLIMIENTO Y ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD (ENS).

El MDEF está comprometido con el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y ha realizado un gran esfuerzo para adecuarse y adaptarse al nuevo marco normativo, alcanzando la conformidad con el ENS en varios sistemas y estableciendo los cambios requeridos en el marco organizativo, operacional y de sistemas.

Tras la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, la publicación del Plan de Transformación Digital de la AGE y sus Organismos Públicos (Estrategia 2015-2020) y la última actualización del ENS (a través del Real Decreto 951/2015, de 23 de octubre), se plantea la necesidad de extender el alcance de la convergencia con el ENS a todos los sistemas de las Administraciones Públicas que no manejen información clasificada. Para ello se deberán establecer medidas organizativas y de gestión y procedimentales, con el fin de impulsar y proseguir la labor de adecuación, de forma que se garantice un determinado nivel de confianza y una protección apropiada de la información y los servicios.

La adecuación al ENS se desarrollará en coordinación con la Política CIS/TIC del MDEF, establecida en la Orden DEF/2639/2015, de 3 de diciembre, y en concreto con el desarrollo de los Objetivos Estratégicos del PECIS. De este modo, el presente Objetivo se orienta hacia la determinación de los planes y actuaciones para la consolidar la adecuación al ENS del MDEF, mientras que la ejecución práctica de dichos planes y actuaciones técnicas se llevará a cabo en el marco del PECIS y su desarrollo, asegurando su alineamiento con el resto de iniciativas que en relación con la racionalización de los medios CIS/TIC se desarrollen en el Departamento.

Líneas de Acción Asociadas:

LA 3.1. Actualizar el Plan de Adecuación al ENS del Ministerio de Defensa con el nuevo alcance (Ley 39/2015 y Ley 40/2015, Estrategia TIC de la AGE), definiendo las responsabilidades que tendrá cada ámbito del nivel específico en la adecuación de sus sistemas.

CVE: BOD-2018-070-8485

LA 3.2. Analizar la aplicación del ENS a los sistemas de información que no afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado, y que no manejen información clasificada de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en Acuerdos Internacionales.

LA 3.3. Analizar la aplicación de las normas del CCN a los sistemas de información que afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado, y que no manejen información clasificada de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en Acuerdos Internacionales.

LA 3.4. Establecer los procedimientos de adecuación al ENS de los sistemas de información y aplicaciones del MDEF.

LA 3.5. Establecer procesos de evaluación continua de los sistemas ya adecuados para garantizar la conformidad con el ENS.

LA 3.6. Establecer los procedimientos de adecuación a las normas del CCN de los sistemas de información y aplicaciones del MDEF.

LA 3.7. Establecer procesos de evaluación continua de los sistemas ya adecuados para garantizar la conformidad con las normas del CCN.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

Este objetivo será desarrollado por el CESTIC, ya que comprende acciones de todas las áreas de seguridad que deben ser coordinadas. Por ello, se actualizará el Plan de Adecuación al ENS de 2013, que incluirá las medidas necesarias para extender el cumplimiento del ENS a todos los sistemas del MDEF. Se establecerán las responsabilidades que tendrá cada ámbito del nivel específico en la adecuación de sus sistemas.

OE 4. INCREMENTAR EL GRADO DE CUMPLIMIENTO Y CONTROL DE LA NORMATIVA DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA EN LAS DISTINTAS ÁREAS DE SEGINFO (PER, DOC, INS, SIT Y EMP).

Según la Ley 9/1968 sobre secretos oficiales (modificada por la Ley 48/1978), en España podrán ser declaradas 'materias clasificadas' aquellas relativas a "asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado". Al mismo tiempo, se consideran «materias objeto de reserva interna» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pudiera afectar a la seguridad del Ministerio de Defensa, amenazar sus intereses o dificultar el cumplimiento de su misión. A efectos de la Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo, las «materias clasificadas» y las «materias objeto de reserva interna» quedan englobadas en el concepto general de «información clasificada».

En el Informe Anual de SEGINFO 2016 presentado al Secretario de Estado de Defensa (SEDEF), que recoge el análisis de la información aportada por los Jefes de Seguridad de la Información de cada ámbito del nivel específico para las diferentes áreas de seguridad de la Información, se observan disfunciones entre el número de entidades que gestionan información clasificada y aquellas que están debidamente habilitadas/acreditadas para ello.

Para garantizar una adecuada protección de las información clasificada, es imprescindible que se cumpla estrictamente la normativa de seguridad de cada una de las áreas, por lo que se deben impulsar medidas que contribuyan a aumentar el grado de habilitaciones de personas y empresas, autorizaciones de instalaciones y acreditaciones de sistemas.

CVE: BOD-2018-070-8486

Este objetivo contemplará igualmente la figura del Servicio de Protección de Materias Clasificadas del MDEF, establecido en las normas decimotercera y decimocuarta de Instrucción 53/2016, de 24 de agosto, del SEDEF, que 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.

Líneas de Acción Asociadas:

LA 4.1. Impulsar medidas para incrementar el número de personas que acceden a información clasificada debidamente habilitadas, minimizando el número de casos de accesos no autorizados y alcanzar una gestión integrada de las Habilitaciones de Seguridad concedidas (Personales, de Empresa, de Establecimiento).

LA 4.2. Impulsar medidas para incrementar el número de instalaciones autorizadas y sistemas acreditados que gestionen y/o almacenen información clasificada adecuadamente, con el fin de minimizar el número de incidentes e incrementar el grado de control sobre los procesos asociados de gestión de información clasificada.

Implantar la estructura de control y gestión de cifra nacional del Ministerio de Defensa, definida en la Instrucción 7/2017, de 16 de febrero, del SEDEF.

LA 4.3. Mejorar los procesos de intercambio de información clasificada entre entidades, impulsando medidas que permitan mejorar sustancialmente el control y la gestión de la información, maximizando el cumplimiento normativo.

Consolidar y evolucionar el Servicio de Protección de Materias Clasificadas del MDEF, en virtud de las distintas necesidades, en lo referente a los elementos de su estructura funcional (Servicio Central, Servicios Generales y Servicios Locales de Protección de Materias Clasificadas).

LA 4.4. Impulsar medidas para mejorar el control de personal de las empresas que acceden a información clasificada, principalmente como consecuencia de su participación en programas, proyectos o contratos clasificados, y el intercambio de información clasificada con aquellas empresas que dispongan de la correspondiente Habilitación de Seguridad de Establecimiento (HSES).

LA 4.5. Impulsar medidas para incrementar la protección de información clasificada en el Área de SEGINFODOC, incluyendo la elaboración y actualización del Catálogo de Materias Clasificadas del MDEF.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

El Plan de Acción de cada área de seguridad, deberá desarrollar este objetivo, incluyendo las medidas de seguridad necesarias para su cumplimiento. El desarrollo de este objetivo se coordinará estrechamente con el PECIS, en todo aquello relativo a la ejecución de las medidas técnicas necesarias para la acreditación de sistemas y el intercambio de información clasificada.

OE 5. IDENTIFICAR MEDIDAS DE PROTECCIÓN PARA AUMENTAR LA SEGINFO DE LOS SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DEL MDEF, TANTO EN EL ÁMBITO PERMANENTE COMO EN EL DESPLEGABLE.

La Instrucción 58/2016 del SEDEF, por la que se aprueba la AG CIS/TIC, identifica las Capacidades CIS/TIC del Departamento.

CVE: BOD-2018-070-8487

En dicha AG CIS/TIC se recoge que la infraestructura única CIS/TIC del Departamento proporcionará un entorno de Servicios CIS/TIC asegurando el tratamiento único de la información a la que accedan los usuarios de un modo ágil, seguro, fiable y sin discontinuidades. Esta infraestructura integrará las Capacidades CIS/TIC actuales y futuras del Ministerio de Defensa y será el resultado de un proceso de transición desde la situación actual que será recogido en el PECIS.

Por otra parte, la infraestructura única debe asegurar la provisión de Servicios CIS/TIC a los diferentes tipos de usuarios del Departamento (consumidores y proveedores de información y gestores de la misma) en todos los emplazamientos, plataformas, puestos de trabajo y operativos en su caso. Así mismo, debe permitir el acceso a los usuarios desde emplazamientos y ubicaciones no pertenecientes al Departamento (redes y usuarios remotos) así como la interacción de usuarios del Departamento con otras organizaciones, nacionales e internacionales, a través de pasarelas y puntos de interconexión de Servicios CIS/TIC debidamente asegurados y normalizados.

Este objetivo se encuentra íntimamente relacionado con el desarrollo de la Política CIS/TIC, dado que las medidas de protección que se identifiquen en su consecución se deberán ejecutar en el marco del desarrollo de los objetivos del PECIS relacionados.

Líneas de Acción Asociadas:

LA 5.1. Evaluar de forma continua el nivel de riesgo del Departamento y proponer nuevos mecanismos de seguridad que contribuyan a reducir el nivel de riesgo (mitigando el impacto de las amenazas y disminuyendo las posibles vulnerabilidades del MDEF).

LA 5.2. Identificar requerimientos y medidas de protección a cubrir con los servicios y sistemas de seguridad CIS/TIC que contribuyan a reducir el nivel de riesgo, en línea con la evaluación desarrollada.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

El Plan de Acción de cada área de seguridad, deberá desarrollar este objetivo, incluyendo las medidas de seguridad necesarias para su cumplimiento teniendo presentes los Objetivos Estratégicos del PECIS relacionados con la SEGINFO.

OE 6. INCREMENTAR EL GRADO DE CONOCIMIENTO DE LA SITUACIÓN EN MATERIA DE SEGINFO DEL DEPARTAMENTO MEDIANTE EL ESTABLECIMIENTO Y MEJORA DE LOS INDICADORES ADECUADOS Y UN PLAN DE AUDITORÍAS.

El propósito de este objetivo es conocer en profundidad la situación de seguridad del Departamento, sus debilidades y fortalezas, las amenazas a las que se enfrenta y en consecuencia el nivel de riesgo, para poder establecer prioridades objetivas en procesos de asignación de potenciales recursos de personal y de equipamiento que permitan racionalizar las inversiones e impulsar la seguridad de la información.

Con este objetivo se mejorará la toma de decisiones sobre posibles vías de actuación para la mejora de la gestión de la seguridad.

Líneas de Acción Asociadas:

LA 6.1. Establecer las métricas e indicadores que mejor representan el nivel de seguridad y de riesgo del Departamento en cada una de las áreas de seguridad de la información.

LA 6.2. Implantar un proceso de recolección de datos distribuido, automatizado y continuo, para conocer el nivel de riesgo lo más actualizado posible a través del cuadro de mando de seguridad de la información.

CVE: BOD-2018-070-8488

LA 6.3. Implantar un proceso de mejora continua, basado en los resultados del cuadro de mando, con el fin de reducir el nivel de riesgo del Departamento

LA 6.4. Fomentar la toma de decisiones estratégicas en seguridad de la información, basándose en los niveles de riesgo obtenidos del cuadro de mando, del informe anual de seguridad y del Plan de Auditorías.

Establecer dicho Plan de Auditorías y obtener capacidades de auditoría en el ámbito de Nivel Corporativo y sobre todos los ámbitos de Nivel Específico.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

El Plan de Acción de cada área de seguridad de la información, deberá desarrollar este objetivo, incluyendo las medidas de seguridad necesarias para su cumplimiento y el Plan de auditorías correspondiente. Para el caso de las capacidades de auditoría en el área de SEGINFOSIT, se desarrollará según lo establecido en el PECIS.

OE 7. IMPULSAR LA CAPACITACIÓN, CONCIENCIACIÓN Y SENSIBILIZACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN.

Este objetivo persigue promover una sólida cultura de seguridad de la información que permita reducir al mínimo el nivel de riesgo y la exposición a amenazas, mediante la adopción de medidas razonables para garantizar la protección de la información. Para ello, es sumamente importante que el personal conozca los riesgos asociados al tratamiento y distribución de la información y cómo mitigarlos, así como la normativa y los procedimientos que han de seguir.

Para lograr este objetivo, habrá que mejorar y diseñar Planes de formación y concienciación que incluyan conferencias sobre sensibilización, la celebración de jornadas sobre seguridad de la información, la realización de cursos genéricos y especializados en la materia.

Líneas de Acción Asociadas:

LA 7.1. Elaborar un plan de formación para mejorar las habilidades y capacidades del personal en materia de seguridad de la información y promover su ejecución.

LA 7.2. Elaborar un plan de concienciación para comunicar y transferir a los usuarios las buenas prácticas que deben de seguir en materia de seguridad de la información y promover su ejecución.

Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

El Plan de Acción de cada área de seguridad de la información, deberá desarrollar este objetivo, incluyendo las medidas de seguridad necesarias para su cumplimiento.

OE 8. CONSTITUIR Y OPTIMIZAR EL FUNCIONAMIENTO DE LA ESTRUCTURA DE GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DEFENSA.

El modelo de Gobierno de la Seguridad de la Información del Ministerio de Defensa, regulado en la Instrucción 53/2016, de 24 de agosto del SEDEF, 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 de su normativa de desarrollo y aplicación.

Está formado por el Consejo de Dirección de la SEGINFO, la Comisión Ejecutiva de la SEGINFO y los Comités de SEGINFO, y permite asegurar, en última instancia, la correcta consecución del objeto de la Política de SEGINFO, así como de los principios básicos que en ella se definen.

CVE: BOD-2018-070-8489

Como consecuencia del desarrollo del PA SEGINFO y para la consecución de sus Objetivos Estratégicos, se deben llevar a cabo una serie de actuaciones que, dado su número y heterogeneidad, deben ser convenientemente coordinadas, controladas y sujetas a seguimiento, a efectos de que todas tengan como fin último alcanzar la protección adecuada, proporcionada y razonable de la Información del Ministerio, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad, tal y como establece el objeto de la Política Corporativa de SEGINFO.

Líneas de Acción Asociadas:

LA 8.1. Constituir y optimizar el funcionamiento de la Estructura de Gobierno de la SEGINFO del MDEF – Comisión Ejecutiva de la SEGINFO.

LA 8.2. Constituir y optimizar el funcionamiento de la Estructura de Gobierno de la SEGINFO – Comités de la SEGINFO.

Se constituirán los Comités de la SEGINFO correspondientes a las diferentes Área de Seguridad de la Información, según lo establecido en la norma decimoquinta 2.c) de la Instrucción 53/2016, de 24 de agosto: Comité de SEGINFOPER, Comité de SEGINFODOC, Comité de SEGINFOINS, Comité de SEGINFOEMP, Comité de SEGINFOSIT.

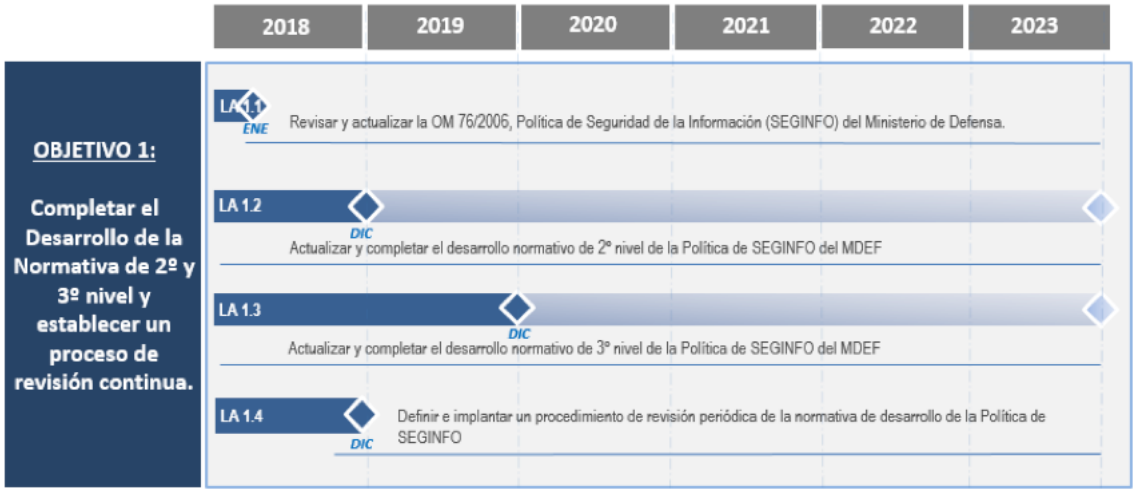
LA 8.3. Definir el procedimiento de coordinación con CESTIC, para el desempeño por este último de las funciones de asistencia y apoyo a las distintas estructuras del Modelo de Gobierno de la SEGINFO.

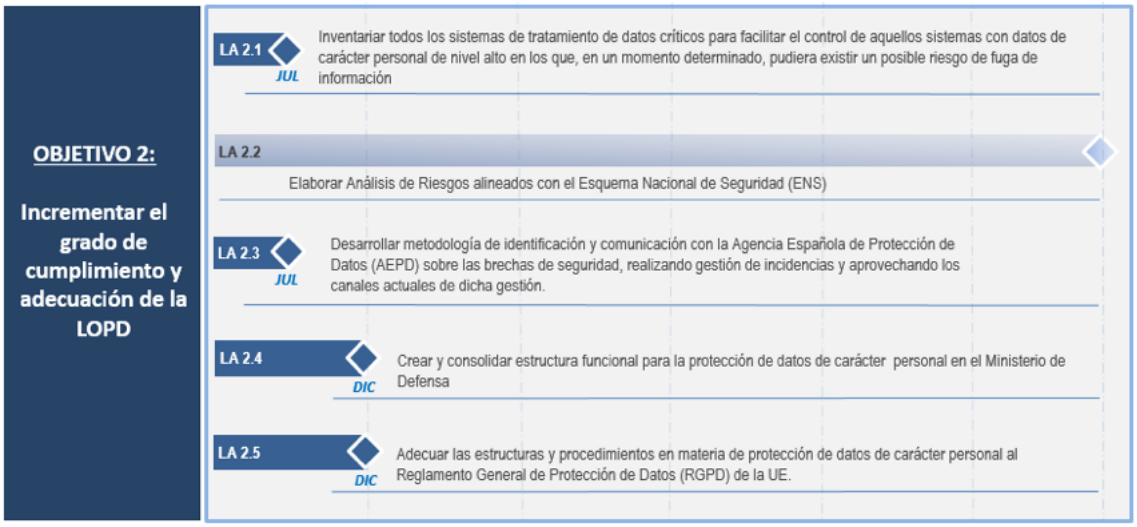
Estrategia de desarrollo del Plan de Acción para la consecución del Objetivo Estratégico.

Dado el carácter de este Objetivo Estratégico y al estar enfocado precisamente a la creación de estructuras que permitan el seguimiento y coordinación de los Planes de Acción que se elaboren, su desarrollo no centralizará en ningún plan de Acción en concreto, sino a través de iniciativas transversales.

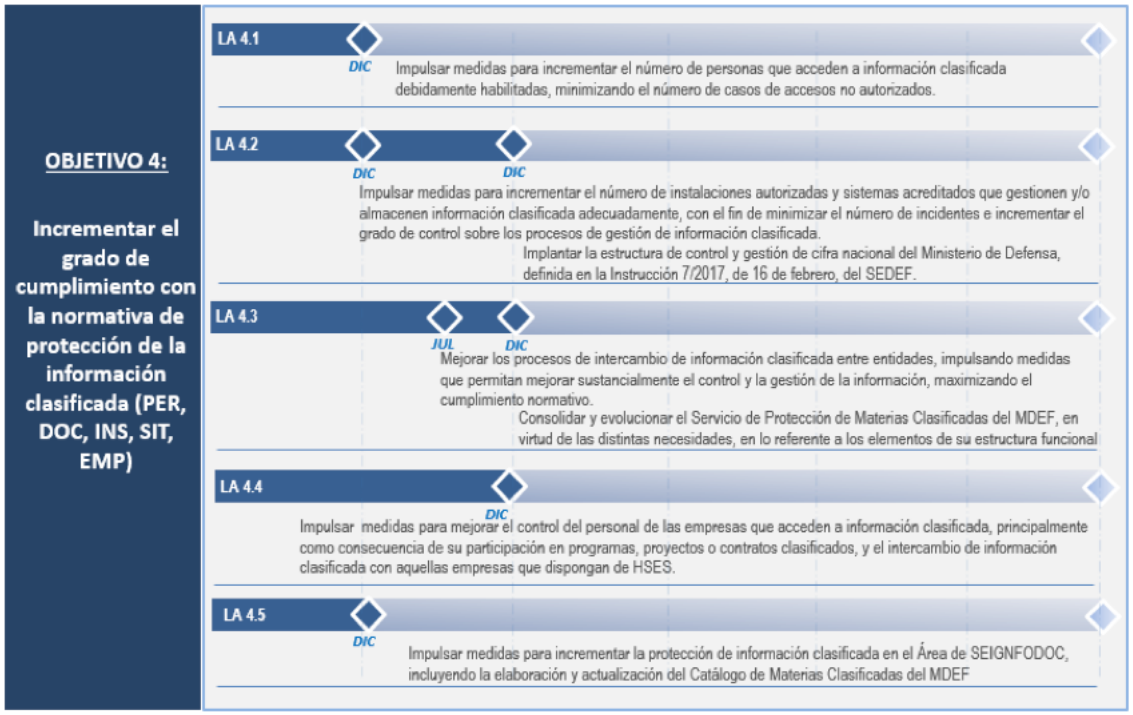
CVE: BOD-2018-070-8490

APÉNDICE I. DIAGRAMA DE GANTT

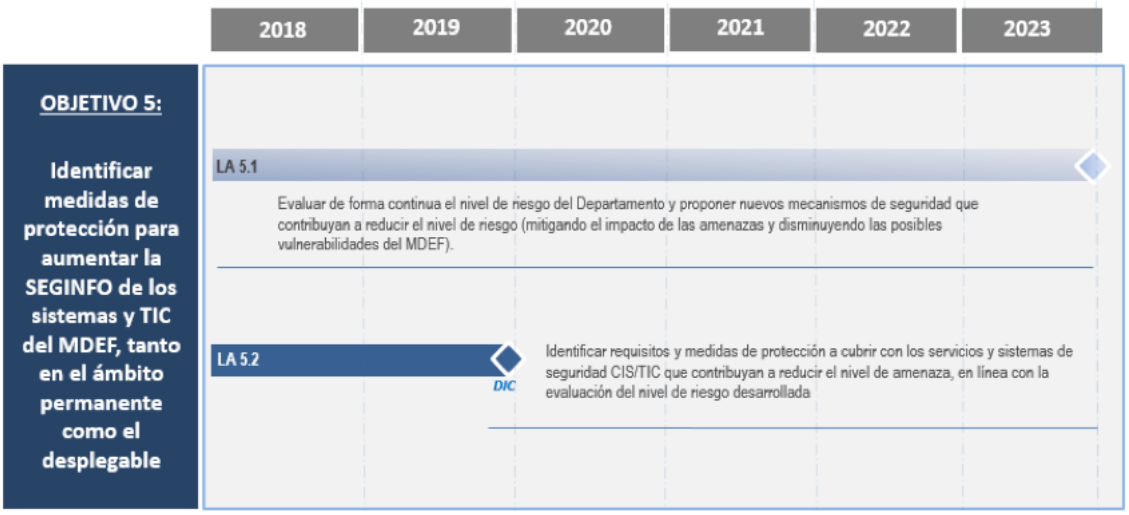


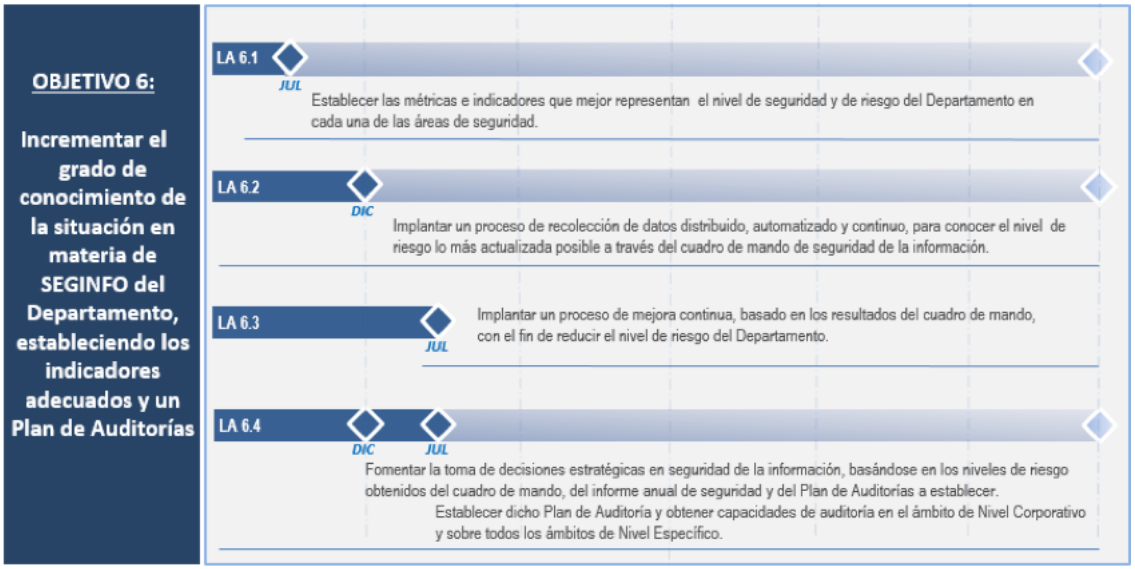


CVE: BOD-2018-070-8491

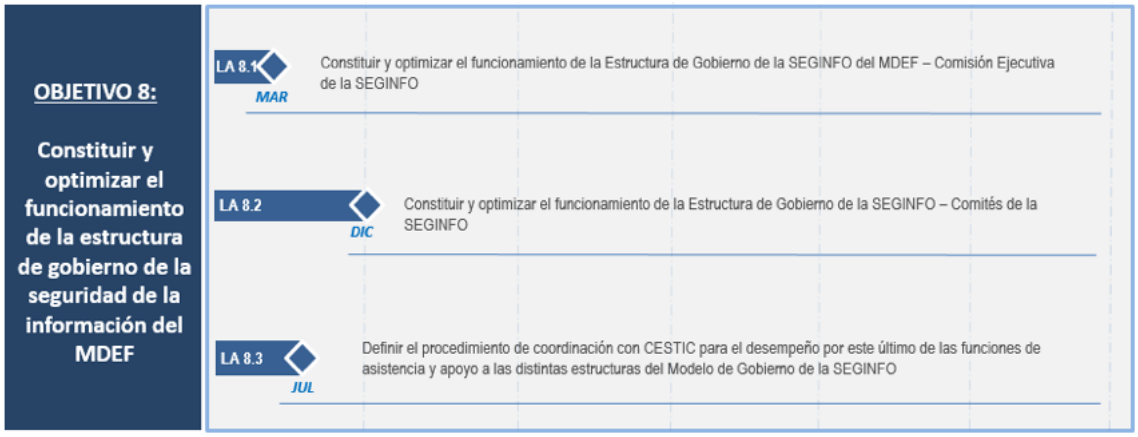


CVE: BOD-2018-070-8492





CVE: BOD-2018-070-8493



CVE: BOD-2018-070-8494

APÉNDICE II. CRITERIOS GENERALES

1. Relaciones entre los órganos de planeamiento y los órganos de ejecución.

La disposición general sexta de la Instrucción 53/2016, especifica que los Responsables de las Áreas de Seguridad de la Información en el nivel corporativo tienen atribuciones sobre la coordinación, y supervisión de las medidas de seguridad de la información en el ámbito del Departamento. Por otra parte en la disposición general séptima, se establece que las atribuciones para la ejecución de las medidas de seguridad las tiene cada ámbito del nivel específico, en las figuras del Responsable de Seguridad de la Información (RSI) y Jefe de Seguridad de la Información (JSI).

Por tanto, teniendo en cuenta lo anterior, en el marco de este plan de actuación y de los futuros planes de acción, los responsables de la implantación de las medidas de seguridad de la información se corresponderán con la estructura funcional de cada ámbito del nivel específico.

En el marco del desarrollo del Plan de Acción General de SEGINFO se concretará, entre otros aspectos, el procedimiento de relación entre los distintos componentes de la Estructura Funcional de la Seguridad de la Información del MDEF, según se establece en la Instrucción 53/2016, de 24 de agosto, del SEDEF: Secretario de Estado de Defensa como Director de Seguridad de la Información del Departamento (DISIDEF), el Director del CESTIC, los Responsables de las Áreas de SEGINFO, los Responsables de Seguridad de la Información en los ámbitos de nivel específico, los Jefes de Seguridad de la Información de los ámbitos de nivel específico y el Servicio de Protección de Materias Clasificadas.

2. Criterios generales para la formación del personal.

El objetivo 7 del presente Plan de Actuación se centra en la concienciación del personal y en la mejora de sus habilidades y capacidades en materia de seguridad de la información, a través de la elaboración de los planes de formación y concienciación, que tratan de acompañarles en su capacidad de desarrollo personal y promoción profesional.

Unos Recursos Humanos suficientes, de calidad, debidamente formados y concienciados, constituyen la piedra angular para ofrecer un adecuado nivel de Seguridad de la Información en el Ministerio de Defensa.

Los Planes de Formación constituyen la herramienta fundamental para la implementación anual de la política formativa del Ministerio de Defensa, e integrarán una formación elaborada a partir de las propuestas realizadas por cada ámbito corporativo, que se encargarán de detectar las necesidades formativas y ejecutar posteriormente dicho Plan, siempre y cuando sea viable en términos económicos y organizativos.

El objetivo principal es garantizar el acceso a la formación del personal como motor de cambio y medio para la mejora continua y actualización de sus conocimientos y capacidades profesionales, así como concienciar y sensibilizar al personal que forma parte del Ministerio de Defensa de la importancia de la Seguridad de la Información. La educación y la formación en seguridad de la información deberán cubrir los siguientes aspectos:

- El compromiso con la seguridad de la información de forma transversal, en toda la organización, que permita al personal establecer medidas de seguridad a aplicar en el desarrollo de sus cometidos.

- El fomento y homogeneización de la formación en Seguridad de la Información en todo el Departamento.

- La necesidad de familiarizarse y cumplir con las normas y obligaciones aplicables en seguridad de la información, según se ha definido en el cuerpo normativo, sensibilizando y concienciando a todo el personal del MDEF, con el fin de maximizar la protección de la información

CVE: BOD-2018-070-8495

• El reconocimiento de las responsabilidades de cada actor, tanto las derivadas de las propias acciones del personal, como las generales orientadas a la securización y protección de la información.

• La difusión de los procedimientos básicos de seguridad de la información (como por ejemplo el proceso para reportar incidentes de seguridad) y controles de línea base tales como seguridad en las contraseñas.

• La identificación y puesta en conocimiento de los puntos de contacto y recursos para obtener información adicional e indicaciones en materias de seguridad de la información.

Todo el personal deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información, en virtud de su perfil y responsabilidades. Los planes de formación y concienciación deberán estar alineados con la Política de Seguridad de la Información y con los procedimientos relevantes, teniendo en consideración la información a proteger y los controles que han sido implementados para proteger dicha información. Así mismo, en el área de SEGINFOST, esta formación se establecerá en el marco del desarrollo de los Objetivos del PECIS en esta materia.

CVE: BOD-2018-070-8496

APÉNDICE III. DIRECTRICES PARA LA TRANSICIÓN DESDE LA SITUACIÓN ACTUAL A LA DESEADA

1. Situación Inicial.

Con el objetivo de conocer la situación actual en materia de seguridad de la información y poder tomar las decisiones adecuadas, el Ministerio de Defensa elabora anualmente un documento en el que se informa sobre el estado de Seguridad de la Información (Informe Anual), así como la situación en materia de protección de datos de carácter personal, en base al análisis de la información aportada por los ámbitos a través de cuestionarios, de la planificación y actuaciones desarrolladas en el nivel corporativo y de las actuaciones desarrolladas por los ámbitos del nivel específico.

Existen algunos casos en los que la calidad de la información no es del todo adecuada. Se ha identificado que estas diferencias se originan en la validación y verificación de los procesos de recopilación de la información, previo a la elaboración de los datos compuestos y estructurados necesarios para la preparación del informe, así como en la realización de procesos complejos de análisis de información, posteriores a la recogida de datos, que aportan un mayor valor al documento.

Se observan las siguientes carencias:

- la justificación y aportación de información adicional que permitan entender las variaciones de tendencia significativas en los datos proporcionados

- la definición e incorporación de indicadores significativos que permitan medir adecuadamente el grado de cumplimiento en relación al estado de la seguridad de la información

- la definición de una metodología de agregación de las fuentes de datos y estandarización de los mismos, que permita elaborar una consolidación del grado de cumplimiento general

- la incorporación de información documentada de los procesos de obtención de los indicadores que se incluyen en los cuestionarios reportados por los distintos ámbitos

- la realización de un proceso de mejora en las medidas de control, validación y revisión de esos datos, con el fin de solventar posibles errores e incoherencias.

Todo ello disminuye la calidad y precisión de la información aportada e impide reflejar debidamente la situación actual de la seguridad de la información con plenas garantías de éxito.

En el marco de este Plan de Actuación, y más en concreto para la consecución del Objetivo 6, se procederá a la implementación de un nuevo enfoque metodológico basado en el análisis estadístico de la información disponible, así como la introducción de nuevas medidas relativas a los procesos de recopilación y análisis de información, que permitan incrementar la fiabilidad del informe anual y establecer una base de análisis que sirva como precedente para el futuro. El análisis estadístico es una herramienta que posibilitará conocer en mayor medida el comportamiento de los datos y permitirá trazar y predecir con cierto grado de solidez tendencias futuras, que permitan adoptar un enfoque reactivo y de anticipación ante condiciones adversas del entorno, y mejorar el grado de conocimiento de la situación actual en materia de seguridad de la información del Ministerio de Defensa.

En base a la información proporcionada en el informe anual, se describe brevemente el grado de cumplimiento actual en las diferentes Áreas de Seguridad de la Información del Departamento. Esta información debe interpretarse y concebirse como una referencia aproximada de la situación actual (téngase en cuenta las citadas diferencias en la calidad de la información).

CVE: BOD-2018-070-8497

Se establece la necesidad de acompañar el desarrollo normativo y de medidas de seguridad con el análisis de la dotación de recursos humanos y económicos necesarios, especialmente cuando conlleva un incremento de las medidas de seguridad, que no puede acometerse con los medios existentes en la actualidad.

Así mismo, todas las áreas precisan respaldar e impulsar planes de formación, concienciación y sensibilización en Seguridad de la Información.

• SEGINFOPER: El área de SEGINFOPER presenta una base sólida en el establecimiento de medidas de seguridad de la información. De forma general, se señalan necesidades relativas a los procesos de renovación de HPS antes de su expiración, y los relacionados con la especificación de requisitos de puestos que manejen información clasificada y su asociación con la necesidad de disposición de HPS, así como el control de esos puestos.

• SEGINFODOC: Esta área también presenta un alto grado de cumplimiento. Se detectan algunas necesidades en el manejo y almacenamiento de documentos clasificados, que debe hacerse siempre en áreas autorizadas adecuadamente, así como en el establecimiento de custodios responsables de la vigilancia y protección de los documentos.

• SEGINFOINS: La falta de dotación económica y humana impacta en mayor medida en el área de SEGINFOINS, debido principalmente a la alta correlación entre la acreditación de Zonas de seguridad (mejora tanto de las medidas físicas como las referentes al control de accesos) y el aumento en el grado de cumplimiento del área.

• SEGINFOSIT: Esta área presenta un alto grado de complejidad a la hora de evaluar y valorar el grado de cumplimiento de los SIT. Se hace necesario incrementar el número de sistemas e interconexiones acreditados, así como el número de auditorías de cumplimiento que permitan conocer en mayor medida si los sistemas cumplen con las políticas y medidas de seguridad establecidas.

En todo caso, en relación a las medidas técnicas, la transición en esta área se desarrollará principalmente de acuerdo con lo establecido en el PECIS y sus Planes de Acción de desarrollo.

• SEGINFOEMP: No se dispone de información actualizada que permita calcular un indicador relacionado con el grado de cumplimiento del área de SEGINFOEMP, ya que este entorno presenta escenarios muy complejos y dispares entre sí. No obstante, se han detectado necesidades de mejora en los siguientes aspectos:

o Disposición de guías de clasificación de los contratos, que permitan mejorar el control de la documentación clasificada generada por las empresas.

o Asignación de Representantes para la seguridad de la información de los contratos, así como inspectores.

o Disposición de las correspondientes Habilitaciones de Seguridad de Empresa (HSEM) por parte de las empresas adjudicatarias, así como Habilitaciones de Seguridad de Establecimiento (HSES), con el fin de disponer de sistemas SIT acreditados y potenciar la entrega de información clasificada en soporte digital.

• LOPD: Existe una herramienta de gestión corporativa de la LOPD (SILOPDEF) que facilita la extracción de indicadores cuantitativos significativos. La versión actual de esta herramienta no permite calcular con un alto grado de precisión el indicador de grado de cumplimiento general, por lo que se están implementando un conjunto de mejoras y actualizaciones con el fin de aumentar la precisión de esta funcionalidad.

CVE: BOD-2018-070-8498

Hasta el momento se ha realizado desde el CESTIC una formación y concienciación en materia de protección de datos a todos los ámbitos, y la Instrucción 16/2017, de 31 de marzo, del Secretario de Estado de Defensa, por la que se aprueban las normas de seguridad de la información que contenga datos de carácter personal en el Ministerio de Defensa, viene a reformar esta función asignada a la unidad.

Durante el 2016 se han realizado auditorías y adecuaciones a diferentes unidades del departamento ofreciendo una fotografía real de cómo se encuentra actualmente el Ministerio de Defensa en esta materia, y la forma en cómo se están aplicando con rigor las medidas de seguridad necesarias según lo dispuesto en la Ley. La Instrucción 16/2017 marca una nueva estructura funcional y, por ende, de trabajo, donde la Unidad LOPD, pasa a denominarse Oficina Central, y actuará de supervisora de las auditorías y adecuaciones que realice cada unidad, tras la formación correspondiente en la materia y el material proporcionado (procedimientos y guías), que servirá de apoyo en su labor.

Queda pendiente la adecuación de la herramienta SILOPDEF y la estructura organizativa a lo establecido en el nuevo Reglamento Europeo de Protección de Datos.

Para obtener una visión elaborada de la situación actual de la seguridad de la información y poder estudiar su evolución a lo largo del tiempo, se precisa disponer de datos o mediciones que sirvan como valores de referencia.

En el ámbito del desarrollo del Objetivo Estratégico 6 de este PA SEGINFO, y más en concreto con la Línea de Acción 6.1 se deben desarrollar conjuntos de métricas que permitan medir el estado, riesgos y nivel de seguridad de los activos, servicios y aplicaciones del Ministerio para facilitar la mejora continua de la calidad de los servicios y de la protección de la información involucrada en cada caso.

En materia de seguridad de la información, dada la gran cantidad de datos disponibles y la transversalidad de la misma afectando a prácticamente cualquier ámbito de actividad, es necesario resumir en una serie limitada de indicadores lo más representativos posibles, sin perjuicio de poder profundizar en ellos cuando fuera requerido un análisis en más detalle.

Teniendo en cuenta esta premisa, la concreción de estas métricas, así como la determinación de los niveles que en cada caso se establezcan como necesarios, se incluirá en los correspondientes Planes de Acción de desarrollo de este PA SEGINFO. Además, para el caso del área de SEGINFOSIT, estas métricas se establecerán igualmente en los Planes de Acción de desarrollo del PECIS.

2. Situación Deseada.

La información es un valioso activo del que depende el buen funcionamiento del Ministerio de Defensa. Mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos planteados. Por esa razón, el Ministerio de Defensa tiene como reto, en un plazo establecido de 6 años, integrar de manera coherente y sistémica, con un enfoque integral y totalizador, la seguridad de la información en todos sus ámbitos.

Al final de ese periodo se deberá alcanzar un nivel de madurez suficiente, donde todos los procesos y medidas aplicadas sean controlados mediante técnicas estadísticas y otras técnicas cuantitativas, y donde se hayan logrado todos los objetivos estratégicos.

La implantación de un Sistema de Gestión de la Seguridad de la Información, gestionado y medible, permitirá acometer con garantía de éxito las misiones encomendadas y cumplir con la legislación vigente en referencia al Esquema Nacional de Seguridad, la protección de datos de carácter personal y en materia de Seguridad de la Información. El sistema está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que permitan proteger de forma adecuada los activos de información del Ministerio de Defensa. Este proceso contemplará las siguientes actuaciones:

CVE: BOD-2018-070-8499

• Desarrollar e implementar un plan de tratamiento del riesgo que permita lograr los objetivos de control identificados, teniendo en consideración la financiación y los recursos humanos disponibles.

• Implementación de los controles de seguridad incluidos en el plan de tratamiento de riesgos, con el fin de satisfacer los objetivos de control, en línea con el desarrollo de los Objetivos Estratégicos del PECIS.

• Definir procesos para medir y evaluar la efectividad de los controles.

• Elaborar programas de formación y capacitación.

• Manejar las operaciones derivadas del establecimiento de los controles.

• Ejecutar procedimientos de monitorización y revisión, con el fin de adoptar un enfoque de mejora continua, teniendo en consideración el nivel de riesgo residual y el riesgo aceptable identificado. Esta actuación se desarrollará en el marco de lo establecido en los Objetivos Estratégicos del PECIS.

• Realización de auditorías internas de forma regular para mantener y mejorar de forma continua la seguridad.

CVE: BOD-2018-070-8500

APÉNDICE IV. DIRECTRICES PARA LOS PLANES DE ACCIÓN DE DESARROLLO DEL PA SEGINFO.

1. Introducción.

El presente PA SEGINFO establece una serie de objetivos estratégicos a medio plazo. Estos objetivos estratégicos y sus líneas de acción serán desarrollados por los Planes de Acción correspondientes bajo responsabilidad de las distintas áreas de seguridad de la información.

Los planes de acción son documentos debidamente estructurados, y por medio de ellos se busca "materializar" los objetivos estratégicos previamente establecidos, dotándoles de un elemento cuantitativo y verificable a lo largo del proyecto.

El Plan de Acción compromete el trabajo de una gran parte del personal del Departamento, estableciendo plazos y responsables y un sistema de seguimiento y monitorización de todas las acciones diseñadas.

2. Definición del Plan de Acción.

Según lo establecido en la Instrucción 53/2016 (norma decimonovena, apdo. c), "Es responsabilidad de la Comisión Ejecutiva 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. También es su cometido dar directrices a los Comités de Seguridad de la Información sobre la ejecución de los citados Planes".

Los Planes de Acción 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.

De este Plan de Actuación derivan los siguientes Planes de Acción:

- Plan de Acción General de SEGINFO.
- Plan de Acción de SEGINFOPER.
- Plan de Acción de SEGINFODOC.
- Plan de Acción de SEGINFOINS.
- Plan de Acción de SEGINFOSIT.
- Plan de Acción de SEGINFOEMP.

3. Elaboración del Plan de Acción.

En la misma Instrucción 53/2016 (norma décima, apdo. c), se indica que es cometido del Responsable de la Áreas de Seguridad de la Información "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".

Por lo tanto, serán los Responsables de cada Área de Seguridad de la Información los encargados de elaborar los Planes de Acción definidos anteriormente. El tiempo de ejecución de dichos Planes será entre uno y tres años.

CVE: BOD-2018-070-8501

4. Control y seguimiento de Plan de Acción.

También en la Instrucción 53/2016 (Norma vigesimoprimera) queda definido que "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.

5. Composición y estructura del Plan de Acción.

Los Planes de Acción han de incluir un conjunto de acciones que permitan cumplir con los objetivos expuestos en este Plan de Actuación mediante el desarrollo de las distintas líneas de acción que igualmente se definen. Además de las actuaciones derivadas de este PA SEGINFO, podrán incluir otros tipos de iniciativas, en aquellos casos en que se identifique como necesario:

• Las iniciativas orientadas a la revisión de la normativa aprobada y la normativa pendiente de aprobación, con la finalidad de verificar la coherencia con lo establecido en la Instrucción 53/2016.

• Las iniciativas que no pudieron ser finalizadas en el Plan de Acción de SEGINFO 2015-2016 y las directrices que han sido determinadas en el IV Consejo de Dirección de Seguridad de la Información, celebrado el 25 de octubre del 2016.

• Las nuevas iniciativas que sean aportadas por los diferentes Responsables de las Áreas de Seguridad de la Información.

La estructura de los Planes de Acción podrá variar dependiendo de los objetivos y recursos de cada una de las áreas. No obstante, a continuación se define un esquema que se usará como referencia para su elaboración:

• Introducción. Este apartado deberá incluir un breve análisis de los aspectos más importantes del plan, explicando las razones o motivaciones que han llevado a su ejecución y cuáles son los objetivos que se pretenden alcanzar, asociándolos a los Objetivos Estratégicos de este PA SEGINFO.

• Ámbito de aplicación. Relación de los órganos y organismos públicos adscritos a los que será de aplicación el Plan de Acción.

• Plazo de ejecución. En línea con lo indicado en el Apartado 2. Alcance de este PA SEGINFO, los diferentes Planes de Acción tendrán un alcance temporal de corto plazo (entre uno y tres años). Tan solo se deberán incluir en el Plan, las acciones que se vayan a desarrollar durante ese periodo, con el fin de asegurar el grado necesario de concreción y certidumbre sobre las mismas.

• Situación actual del Área de Seguridad. Descripción de alto nivel del estado de la seguridad de la información del área objeto de cada Plan de Acción.

CVE: BOD-2018-070-8502

• Conjunto de acciones. Por cada uno de los objetivos del Plan de Actuación que aplique a cada área, se detallarán el conjunto de acciones que permitan desarrollar las distintas líneas de acción. Por cada acción se incluirá:

– Título. Nombre descriptivo de la acción.

– Descripción. Exposición detallada de la acción y los aspectos más importantes que contempla. Entre ellos se recogerán las líneas de acción establecidas en el presente documento a las que responde cada acción.

– Ámbito / Área: Indica el Área de la Seguridad de la Información a la que afecta la acción.

– Alcance. Relación de los órganos, unidades y organismos públicos adscritos del Departamento a los que hace referencia la acción, así como aquellos actores externos involucrados en su desarrollo.

– Formación Requerida: Conocimientos previos necesarios para poder abordar la acción.

– Necesidades de personal. Recursos humanos necesarios para el desarrollo de cada acción. En la medida en que varias acciones tengan una alta interrelación, la estimación de las necesidades de personal para su desarrollo podrá abordarse de manera conjunta.

– Necesidades económicas. Recursos financieros necesarios para el desarrollo de cada acción. Nuevamente en la medida en que varias acciones tengan una alta interrelación, la estimación de las necesidades de personal para su desarrollo podrá abordarse de manera conjunta.

– Recursos Materiales. Equipamiento necesario para el desarrollo de cada acción. Del mismo modo que se ha destacado para el caso de los recursos de personal y financieros, se podrán establecer estimaciones de necesidades de recursos materiales conjuntas para varias acciones.

– Planificación Temporal: Tiempo de ejecución mínimo para completar el desarrollo de la acción.

– Responsable de Elaboración. Persona u organismo encargado de elaborar cada una de las acciones.

– Responsable de Aprobación. Persona u organismo encargado de aprobar el Plan de Acción.

– Otros criterios. Criterios de aplicación, directrices de transición o directrices del Plan de Acción que afecten a la acción.

• Prioridades. Se ordenará el conjunto de acciones en base a las prioridades funcionales identificadas por el responsable del plan de acción.

• Cronograma de actividades. De acuerdo con la planificación temporal establecida para cada acción, el plan de acción deberá contener un cronograma detallado de las actividades, que muestre las principales tareas en las que se desglosen y sus asignaciones, así como su tiempo de cumplimiento.

• Memoria de recursos humanos. Atendiendo a las estimaciones de necesidades de recursos humanos necesarios para el desarrollo de cada acción, se elaborará una memoria de las necesidades de personal para el desarrollo del Plan de Acción.

• Memoria de recursos financieros. Atendiendo a las estimaciones de necesidades de recursos financieros necesarios para el desarrollo de cada acción, se elaborará una memoria de las necesidades económicas para el desarrollo del Plan de Acción.

CVE: BOD-2018-070-8503

• Establecimiento de un marco de seguimiento y evaluación del Plan de Acción. Definición de un conjunto de indicadores/métricas que permitan medir el grado de cumplimiento del Plan de Acción.

Cada plan de acción incluirá indicadores que permita evaluar el grado de cumplimiento del mismo.

CVE: BOD-2018-070-8504

APÉNDICE V. NECESIDADES DE RECURSOS HUMANOS

Los recursos humanos propios del MDEF en materia de Seguridad de la Información son un factor crítico para el cumplimiento de los objetivos propuestos en este Plan, y requieren del dimensionamiento adecuado en relación con la función a desempeñar y los hitos marcados, que no debería limitarse a la mera gestión y seguimiento de los recursos contratados, sino constituir el factor fundamental para el desarrollo y culminación de los objetivos del Plan de Actuación.

Los recursos humanos necesarios para el cumplimiento de los objetivos estratégicos de este PA SEGINFO, se obtendrán a partir de las memorias de recursos humanos desarrolladas en los correspondientes planes de acción, tal y como se ha indicado en el Apéndice IV de este PA SEGINFO.

CVE: BOD-2018-070-8505

APÉNDICE VI. NECESIDADES DE RECURSOS FINANCIEROS

Para acometer los objetivos planteados en el presente Plan será preciso adoptar mecanismos de financiación de las inversiones necesarias.

Los recursos financieros necesarios para el cumplimiento de los objetivos estratégicos de este PA SEGINFO, se obtendrán a partir de las memorias económicas desarrolladas en los correspondientes planes de acción.

CVE: BOD-2018-070-8506

APÉNDICE VII. NORMATIVA DE APLICACIÓN

[1] OM 76/2006, del 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa.

[2] 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.

[3] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[5] Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

[6] Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones.

[7] Plan Estratégico de Sistemas y Tecnologías de Información y Comunicaciones (PECIS).

[8] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo LOPD.

[9] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[10] Instrucción 16/2017, de 31 de marzo, del Secretario de Estado de Defensa, por la que se aprueban las normas de seguridad de la información que contenga datos de carácter personal.

[11] Plan de Transformación Digital de la AGE y sus organismos públicos (Estrategia TIC 2015 – 2020), aprobada por el Consejo de Ministros el 2 de octubre de 2015.

[12] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

[13] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

[14] Ley 9/1968, de 5 de abril (BOE. Núm. 84, de 6 de Abril de 1968), modificada por la Ley 48/1978, de 7 de octubre (BOE. Núm. 243) sobre Secretos Oficiales.

[15] Instrucción 22/2016, de 11 de abril, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información en las Personas (SEGINFOPER).

[16] 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 (SEGINFOINS).

[17] Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos (SEGINFODOC).

[18] Instrucción 52/2013, de 17 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la información en poder de las Empresas (SEGINFOEMP).

CVE: BOD-2018-070-8507

[19] Instrucción 64/2015, de 7 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información para la elaboración, clasificación, cesión, distribución y destrucción de información del Ministerio de Defensa.

[20] Instrucción 7/2017, de 16 de febrero, del Secretario de Estado de Defensa, por la que se establece la estructura funcional para la gestión y el control del material de cifra nacional del Ministerio de Defensa.

CVE: BOD-2018-070-8508

APÉNDICE VIII. ABREVIATURAS Y ACRÓNIMOS

- AEPD: Agencia Española de Protección de Datos.
- CCN: Centro Criptológico Nacional.
- CNI: Centro Nacional de Inteligencia.
- CESTIC: Centro de Sistemas y Tecnologías de la Información y las Comunicaciones.
- DISIDEF: Director de Seguridad de la Información del Ministerio de Defensa.
- ENS: Esquema Nacional de Seguridad.
- HPS: Habilitación Personal de Seguridad.
- HSEM: Habilitación de Seguridad de Empresa.
- HSES: Habilitación de Seguridad de Establecimiento.
- JSI: Jefe de Seguridad de la Información.
- LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- MDEF: Ministerio de Defensa.
- PECIS: Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones.
- Política CIS/TIC: Política de los Sistemas y Tecnologías de la Información y las Comunicaciones.
- RGPD: Reglamento General de Protección de Datos de la Unión Europea.
- RSI: Responsable de Seguridad de la Información.
- SEDEF: Secretario de Estado de Defensa.
- SEGINFO: Seguridad de la Información.
- SEGINFODOC: Seguridad de la Información en los Documentos.
- SEGINFOEMP: Seguridad de la Información en poder de las Empresas.
- SEGINFOINS: Seguridad de la Información en las Instalaciones.
- SEGINFOPER: Seguridad de la Información en las Personas.
- SEGINFOSIT: Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.

CVE: BOD-2018-070-8509