



BOD

BOLETÍN OFICIAL DEL MINISTERIO DE DEFENSA

AÑO XL

VIERNES, 2 DE AGOSTO DE 2024

NÚMERO 152

SUMARIO

I. — DISPOSICIONES GENERALES

Página

MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

Real Decreto 759/2024, de 30 de julio, por el que se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

22649

III. — PERSONAL

DIRECCIÓN GENERAL DE PERSONAL

PERSONAL MILITAR

Vacantes	22650
Destinos	22652
Nombramientos	22664

**CUERPOS COMUNES DE LAS FUERZAS ARMADAS**

CUERPO MILITAR DE INTERVENCIÓN

• ESCALA DE OFICIALES

Ascensos 22665

CUERPO MILITAR DE SANIDAD

• ESCALA DE OFICIALES

Destinos 22666

• ESCALA DE OFICIALES ENFERMEROS

Ascensos 22667

CUERPO DE MÚSICAS MILITARES

• ESCALA DE SUBOFICIALES

Ascensos 22669

EJÉRCITO DE TIERRA

CUERPO GENERAL

• ESCALA DE OFICIALES

Servicio activo 22670

Destinos 22671

Comisiones 22673

• ESCALA DE SUBOFICIALES

Servicio activo 22674

Retiros 22676

Suspensión de funciones 22677

• ESCALA DE TROPA

Servicio activo 22679

Excedencias 22681

Bajas 22682

Ceses 22690

Suspensión de funciones 22692

Destinos 22696

VARIOS CUERPOS

Destinos 22698

RESERVISTAS

Situaciones 22700

ARMADA

CUERPO GENERAL

• ESCALA DE OFICIALES

Destinos 22701

• ESCALA DE SUBOFICIALES

Servicio activo 22702

• VARIAS ESCALAS

Destinos 22704

CUERPO DE INFANTERÍA DE MARINA

• ESCALA DE OFICIALES

Ascensos 22707

Destinos 22709

**EJÉRCITO DEL AIRE Y DEL ESPACIO****CUERPO GENERAL**

- ESCALA DE OFICIALES
 - Ascensos 22711
 - Destinos 22718
 - Comisiones 22726
 - Recompensas 22727
- ESCALA DE SUBOFICIALES
 - Ascensos 22728
- ESCALA DE TROPA
 - Bajas 22729
 - Licencia por asuntos propios 22730
 - Licencia por estudios 22731
 - Vacantes 22732
 - Destinos 22733

CUERPO DE INTENDENCIA

- MILITARES DE COMPLEMENTO
 - Destinos 22734

CUERPO DE INGENIEROS

- ESCALA DE OFICIALES
 - Nombramientos 22735

GUARDIA CIVIL**ESCALA DE OFICIALES**

- Ascensos 22736

ESCALA DE CABOS Y GUARDIAS

- Retiros 22737

IV. — ENSEÑANZA MILITAR**ENSEÑANZA DE FORMACIÓN**

- Bajas de alumnos 22738

V. — OTRAS DISPOSICIONES

- PREMIOS 22739

MINISTERIO DE DEFENSA

- DELEGACIÓN DE COMPETENCIAS 22740
- SEGURIDAD INFORMÁTICA 22742
- ZONAS DE INTERÉS PARA LA DEFENSA NACIONAL 22757

MINISTERIO DE HACIENDA

- SECTOR PÚBLICO ESTATAL. CUENTAS ANUALES 22761



RETRIBUCIONES

ARMADA

CUERPO DE INFANTERÍA DE MARINA

- ESCALA DE SUBOFICIALES

Trienios 22762

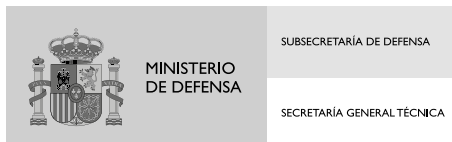
AVISO LEGAL.

«1. El «Boletín Oficial del Ministerio de Defensa» es una publicación de uso oficial cuya difusión compete exclusivamente al Ministerio de Defensa. Todos los derechos están reservados y por tanto su contenido pertenece únicamente al Ministerio de Defensa. El acceso a dicho boletín no supondrá en forma alguna, licencia para su reproducción y/o distribución, y que, en todo caso, estará prohibida salvo previo y expreso consentimiento del Ministerio de Defensa.

2. El «Boletín Oficial del Ministerio de Defensa», no es una fuente de acceso público en relación con los datos de carácter personal contenidos en esta publicación oficial; su tratamiento se encuentra amparado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. De conformidad con la citada ley orgánica queda terminantemente prohibido por parte de terceros el tratamiento de los datos de carácter personal que aparecen en este «Boletín Oficial del Ministerio de Defensa» sin consentimiento de los interesados.

3. Además, los datos de carácter personal que contiene, sólo se podrán recoger para su tratamiento, así como someterlos al mismo, cuando resulten adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, de acuerdo con el principio de calidad.»

Edita:



Diseño y Maquetación:
Imprenta del Ministerio de Defensa

**I. — DISPOSICIONES GENERALES****MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES
CON LAS CORTES****ORGANIZACIÓN**

Cód. Informático: 2024018264. (Del BOE núm. 184, de 31-7-2024) (B. 152-1)

Real Decreto 759/2024, de 30 de julio, por el que se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

<https://www.boe.es/boe/dias/2024/07/31/pdfs/BOE-A-2024-15702.pdf>



V. — OTRAS DISPOSICIONES

PREMIOS

Resolución 600/12341/24

Cód. Informático: 2024018087.

Resolución del Almirante Jefe de Estado Mayor de la Armada, por la que se conceden los premios de la Revista General de Marina del año 2023.

El apartado segundo de la Instrucción 2/2014, de 8 de enero de 2014, del Jefe de Estado Mayor de la Armada, por la que se establecen las normas para la concesión de los premios «Revista General de Marina» de la Armada, fija las distintas modalidades de premios y su finalidad.

Una vez finalizados los trabajos de selección de la Junta Calificadora, aprobado el gasto necesario para el pago de los premios con dotación económica objeto de la presente Resolución (7.180 euros, con cargo a la aplicación presupuestaria 14.17.121M2.226.09), y tras la tramitación del correspondiente expediente en los términos previstos por la Ley 47/2003, de 26 de noviembre, procede la concesión de los premios correspondientes al año 2023, conforme a la citada Instrucción.

En su virtud y a propuesta de la Junta Calificadora de los premios «Revista General de Marina»,

RESUELVO:

Primero: Se conceden los premios que a continuación se relacionan a los autores de los artículos cuyo título se indica:

- Premio «Álvaro de Bazán», dotado con 2.100 €, al AN (CGA) Álvaro Babé Pérez de Villar, por su artículo: «Drones: El papel que están teniendo en la guerra moderna».
- Premio «Roger de Lauria», dotado con 1.650 €, al CF (CGA) Francisco Díaz Rodríguez, por su artículo: «Informes personales Vs. Inteligencia emocional».
- Premio «Francisco Moreno», dotado con 1.330 €, al CN (CGA) (R) Fernando Bandín Saura, por su artículo: «El mando es el mando».
- Premio «Antonio de Oquendo», concedido ex aequo, dotado con 1.050 € para cada uno de los dos premiados, al CF (CGA) Ignacio Carvajal Cervera, por su artículo «La gestión estratégica del talento» y al CC (ING) Juan Manuel de Santiago Collada, por su artículo «Defensa antimisil (o sobre cómo ganar mundiales de fútbol en los penaltis)».
- Diploma acreditativo RGM, sin dotación económica, al Dr. D. Luis Vicente Pérez Gil.

Segundo: A los galardonados se les hará entrega de los diplomas acreditativos de los premios, así como de su correspondiente asignación en metálico.

Tercero: La presente Resolución de concesión pone fin a la vía administrativa, pudiéndose interponer recurso potestativo de reposición ante mi Autoridad, en el plazo de un mes contado a partir del día siguiente al de su publicación.

Madrid, 29 de julio de 2024.—El Almirante Jefe de Estado Mayor de la Armada, Antonio Piñeiro Sánchez.



V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

DELEGACIÓN DE COMPETENCIAS

Cód. Informático: 2024018269. (Del BOE núm. 184, de 31-7-2024) (B. 152-2)

Resolución 560/38324/2024, de 22 de julio, de la Jefatura del Mando de Personal del Ejército de Tierra, sobre delegación de competencias.

La Orden Ministerial 2/2023, de 25 de enero («Boletín Oficial de Defensa» número 23), por la que se aprueban las instrucciones para la aplicación en las Fuerzas Armadas del Reglamento de Armas, en el apartado 3 de su Capítulo III, atribuye al General Jefe del Mando de Personal del Ejército de Tierra la competencia para apreciar la necesidad de portar las armas amparadas por las licencias tipo «A» por razones de seguridad, referido a la prohibición de portar, exhibir y usar fuera del domicilio, del lugar de trabajo, en su caso, o de las correspondientes actividades deportivas cualquier clase de armas de fuego cortas, a los efectos de lo dispuesto en el artículo 146 del Real Decreto 137/1993, de 29 de enero («Boletín Oficial del Estado» número 55), por el que se aprueba el Reglamento de Armas.

No obstante, se sigue considerando que determinadas autoridades dependientes directamente del Jefe de Estado Mayor del Ejército de Tierra disponen de los elementos de juicio y la capacidad de mando necesaria para ejercer la potestad que se les confiere en esta delegación.

En su virtud, previa aprobación del Jefe de Estado Mayor del Ejército de Tierra, en uso de las facultades que me confiere el artículo 9 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispongo:

Primero. *Delegación de competencias.*

1. Se delega en las siguientes autoridades las atribuciones que actualmente tiene conferidas el General Jefe del Mando de Personal por el apartado 3, del Capítulo III de la Orden Ministerial 2/2023, de 25 de enero, por la que se aprueban las instrucciones para la aplicación en las Fuerzas Armadas del Reglamento de Armas, para apreciar la necesidad de portar las armas amparadas por las licencias tipo «A» por razones de seguridad, referido a la prohibición de portar, exhibir y usar fuera del domicilio, del lugar de trabajo, en su caso, o de las correspondientes actividades deportivas cualquier clase de armas de fuego cortas, a los efectos de lo dispuesto en el Reglamento de Armas, respecto del personal militar encuadrado orgánicamente en las unidades dependientes de estos:

- General Jefe del Cuartel General Terrestre de Alta Disponibilidad.
- General Jefe de la Fuerza Terrestre.
- General Jefe del Mando de Canarias.
- General Jefe del Mando de Adiestramiento y Doctrina.
- General Jefe del Mando de Apoyo Logístico.
- General Jefe de la Inspección General del Ejército.
- General Jefe de la Jefatura del Ciberespacio y de los Servicios de Asistencia Técnica del ET.
- General Jefe del Instituto de Historia y Cultura Militar.
- General Jefe de la Dirección de Asuntos Económicos.

2. Se delega esta misma competencia, para el personal militar del Ejército de Tierra perteneciente al Cuartel General del Ejército, excepto el encuadrado en la Jefatura del Ciberespacio y de los Servicios de Asistencia Técnica del ET y en el Instituto de Historia y Cultura Militar, en el General Segundo Jefe de Estado Mayor del Ejército.

**Segundo. Antefirma.**

Las resoluciones administrativas que se adopten en virtud del apartado anterior indicarán expresamente esta circunstancia, haciendo constar en la antefirma la expresión «Por delegación», con referencia a esta resolución.

Tercero. Avocación.

En todo momento, y mediante acuerdo motivado, mi autoridad podrá avocar para sí el conocimiento y resolución de cualquier asunto de la delegación que se otorga en la presente resolución, de conformidad con lo previsto en el artículo 10 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Cuarto. Efectos.

La presente resolución producirá efectos a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

Madrid, 22 de julio de 2024.–El General Jefe del Mando de Personal del Ejército de Tierra, Antonio Jesús Cabrerizo Calatrava.



V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA SEGURIDAD INFORMÁTICA

Cód. Informático: 2024018271. (Del BOE núm. 184, de 31-7-2024) (B. 152-3)

Orden DEF/807/2024, de 22 de julio, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.

La información es un recurso estratégico del Ministerio de Defensa, fundamental para facilitar el cumplimiento de las misiones y los cometidos encomendados al departamento. De ella dependen todos los procesos del Ministerio de Defensa, razón por la cual debe ser organizada y controlada a lo largo de su ciclo de vida, independientemente del medio y del formato en el que se encuentre.

La política de seguridad de la información del Ministerio de Defensa, aprobada por la Orden Ministerial 76/2006, de 19 de mayo, así como su desarrollo posterior, han establecido el marco normativo necesario para alcanzar la protección adecuada, proporcionada y razonable de dicha información, mediante la preservación de los requisitos mínimos de seguridad que afectan a su confidencialidad, integridad y disponibilidad. Asimismo, la actualización de dicha política responde a la constante evolución del entorno, en particular de los riesgos y amenazas y de la evolución de los sistemas y tecnologías de la información y las comunicaciones, lo que exige dotar al Ministerio de Defensa de una estructura que incorpore la seguridad de manera inherente a los servicios CIS/TIC, en línea con la Estrategia Nacional de Ciberseguridad, aprobada en su última versión en 2019 por el Consejo de Seguridad Nacional. Esta actualización debe contemplar los conceptos y estructuras que forman parte de la cultura de seguridad de la información del Ministerio de Defensa, mejorando su adecuación a su organización, en función de su especificidad en los ámbitos de la preparación de la Fuerza y de las operaciones militares.

Consecuentemente, desde la aprobación de la citada Orden Ministerial 76/2006, de 19 de mayo, en el ámbito del Ministerio de Defensa se han aprobado diferentes normas que persiguen garantizar la eficacia, eficiencia y seguridad de la información, atendiendo a las condiciones específicas de dicho departamento ministerial. Entre los aspectos más destacado, se puede citar, entre otros, la aportación, por parte del Mando Conjunto del Ciberespacio (MCCE), del Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa (ESPDEF-CERT) al contexto de la ciberseguridad nacional, posible gracias a la aprobación de la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas; la generación de capacidades de Seguridad de la Información de la infraestructura CIS/TIC del departamento, a fin de satisfacer las necesidades CIS/TIC de las Fuerzas Armadas en la toma de decisiones y conducción de las operaciones, asegurando la autoridad del Jefe de Estado Mayor de la Defensa (JEMAD) sobre la I3D en el ámbito operativo en virtud de los acuerdos específicos suscritos al efecto entre dicha autoridad y la persona titular de la Secretaría de Estado de Defensa (SEDEF), mediante la 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, y su desarrollo mediante la Arquitectura Global CIS/TIC y el Plan Estratégico CIS; la trascendencia y transversalidad de los Sistemas y Tecnologías de la Información y las Comunicaciones, en consonancia con lo establecido en la Orden Ministerial 5/2017, de 9 de febrero, por la que se aprueba la Política de gestión de documentos electrónicos del Ministerio de Defensa, que regula la gestión de documentación electrónica, activo de información especialmente relevante por su volumen, frecuencia de uso, número de usuarios, posibilidades en su manejo y transferencia; y la protección de la información aplicando las medidas necesarias para garantizar su disponibilidad, integridad y confidencialidad a lo largo de todo su ciclo de



vida, conforme lo dispuesto la Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa.

El desarrollo normativo anteriormente citado está en línea con las exigencias establecidas en el marco de la Administración General del Estado, conforme a lo dispuesto en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referente al Esquema Nacional de Interoperabilidad (ENI) y al Esquema Nacional de Seguridad (ENS). El ENS, de obligado cumplimiento por el Ministerio de Defensa, establece los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. Asimismo, exige que cada administración pública cuente formalmente con una política de seguridad que disponga del conjunto de directrices que rigen la forma en que esa organización gestiona y protege la información que trata y los servicios que presta, debiendo ser aprobada dicha política por la persona titular del Departamento. En este marco, se ha incorporado la figura del Responsable Funcional (RFUN), que integra la figura del Responsable de la Información y del Responsable del Servicio en el Ministerio de Defensa.

Por otra parte, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que establece un sistema de notificación de incidentes, se desarrolla mediante el Real Decreto 43/2021, de 26 de enero, cuyo ámbito de aplicación son los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas. Sin embargo, el ámbito de aplicación de dicha ley exceptúa explícitamente las infraestructuras dependientes del Ministerio de Defensa, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos. La presente política de seguridad de la información tiene en cuenta lo anterior y establece el marco necesario para desarrollar la normativa y procedimientos específicos de seguridad de las redes y sistemas de información del departamento y para que el ESPDEF-CERT del MCCE sea el de referencia del Ministerio de Defensa.

La presente política de seguridad de la información que se aprueba por esta orden ministerial, en línea con las normas anteriormente citadas, establece el marco necesario para establecer aspectos específicos de seguridad de las redes y sistemas de información del Ministerio de Defensa, del que emanará toda la normativa interna en materia de seguridad de la información del departamento, facilitando así la necesaria coordinación en el desarrollo normativo posterior para alcanzar un conjunto normativo equilibrado, completo y con criterios unificados, incluyendo las normas de seguridad de la información que contengan datos de carácter personal del Ministerio de Defensa, de acuerdo con lo dispuesto en el 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; así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. A tal efecto, se incorpora como una nueva área de seguridad de la información, de forma que se preserve también este derecho fundamental de las personas físicas.

El Real Decreto 205/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, atribuye en su artículo 3 a la Secretaría de Estado de Defensa, entre otras funciones, la dirección, impulso y gestión de la política de seguridad de la información en el ámbito de la Defensa. Asimismo, en su artículo 7 asigna al Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) la definición y planificación de las políticas y estrategias relativas a los sistemas y tecnologías de la información y las comunicaciones, la transformación digital y seguridad de la información, así como su desarrollo y actualización, la coordinación de



su ejecución y control de su cumplimiento, así como la responsabilidad del sistema y de la seguridad sobre los sistemas de información de la I3D, según lo establecido en el artículo 13 del ENS.

De la presente política de seguridad de la información en el Ministerio de Defensa emanan todas las directrices internas en materia de seguridad de la información del departamento, a fin de alcanzar un conjunto de disposiciones equilibrado, completo y con criterios unificados. Todo ello, sin menoscabo de lo dispuesto en la Ley Orgánica 05/2005, de 17 de noviembre, de la Defensa Nacional, que salvaguarda la responsabilidad plena del JEMAD sobre la estructura operativa de las Fuerzas Armadas en las actividades y las operaciones militares, en cumplimiento de sus competencias para asegurar su eficacia operativa, incluyendo lo relativo a la seguridad de la información, supervisando la preparación de las unidades de la fuerza y evaluando su disponibilidad operativa. Las disposiciones emanadas de esta Política y del cuerpo normativo que la desarrolle no podrán comprometer el cumplimiento de las misiones de las Fuerzas Armadas ni la seguridad operativa de una operación militar.

Esta orden ministerial es coherente con los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Los principios de necesidad y eficacia quedan salvaguardados ya que la iniciativa está justificada por razones de interés general con el fin de contar con un marco normativo actualizado que regule la política de seguridad de la información en el ámbito del Ministerio de Defensa. Asimismo, queda claramente identificado el fin perseguido de disponer de una norma que regule esta materia. En cuanto al principio de proporcionalidad, se trata de una disposición que pretende facilitar la gestión, tratando de contener la regulación imprescindible. Respecto del principio de seguridad jurídica, la norma es coherente con el resto del ordenamiento jurídico nacional y ofrece un marco normativo estable. Desde la perspectiva del principio de transparencia, se han definido claramente los objetivos. Por último, la orden ministerial evita cargas administrativas accesorias o innecesarias y es racionalizadora porque su aprobación potencia el empleo de los medios electrónicos en el proceso de gestión, de forma que resulta acorde con el principio de eficiencia.

En su virtud, y de acuerdo con lo dispuesto en el artículo 61 letra a) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispongo:

Artículo 1. Aprobación de la política de seguridad de la información.

Se aprueba la política de seguridad de la información del Ministerio de Defensa, cuyo texto se anexa a continuación.

Artículo 2. Dirección de la seguridad de la información del Ministerio de Defensa.

La persona titular de la Secretaría de Estado de Defensa asumirá la responsabilidad de Director de Seguridad de la Información del Ministerio de Defensa, encomendándole, en el ámbito del Ministerio de Defensa, la dirección, impulso y gestión de la política de seguridad de la información, así como la definición y la creación de la estructura funcional de la seguridad de la información, incluyendo en esta última el Servicio de Protección de Materias Clasificadas.

Artículo 3. Protección de datos de carácter personal.

Corresponde al delegado de Protección de Datos (DPD) del Ministerio de Defensa informar y asesorar a los Responsables del Tratamiento (RT) de las obligaciones que les incumben en virtud del 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), además de supervisar el cumplimiento de la normativa en materia de protección de datos



de carácter personal del departamento, ofrecer asesoramiento y actuar como interlocutor de los RT con la Agencia Española de Protección de Datos (AEPD).

Artículo 4. *Protección de materias clasificadas.*

Corresponde a la persona titular de la Dirección del Centro Nacional de Inteligencia (CNI) velar por el cumplimiento de la normativa relativa a la protección de materias clasificadas.

Artículo 5. *Control de Material de Cifra.*

1. Corresponde a la persona titular de la Autoridad de Control de Material de Cifra (ACMC) velar por la correcta gestión y control del material de cifra nacional del departamento.

2. Corresponde a la persona titular de la Agencia Nacional de Distribución de Material Cifra (ESP NDA) velar por la correcta gestión y control del material de cifra no nacional.

Disposición adicional primera. *Servicio de Protección de Materias Clasificadas del CNI.*

El Centro Nacional de Inteligencia, atendiendo a su misión y funciones legalmente establecidas, dispondrá de su propio Servicio de Protección de Materias Clasificadas, denominado Servicio de Protección de Información Clasificada, bajo la dependencia directa de su Secretario General, según se establece en su normativa reguladora.

Disposición adicional segunda. *Información de la jurisdicción militar.*

La información que pueda figurar en los distintos procedimientos de la jurisdicción militar se registrará exclusivamente por su normativa específica.

Disposición adicional tercera. *Seguridad de la información procedente de terceros y organismos ajenos al Ministerio de Defensa.*

1. La información suministrada al Ministerio de Defensa por organizaciones internacionales o países extranjeros tendrá el tratamiento y limitaciones concretas que impongan los acuerdos o tratados, convenios bilaterales o multilaterales en los que España sea parte y a cuyo amparo haya sido facilitada dicha información.

2. La información suministrada al Ministerio de Defensa por otros órganos de las Administraciones Públicas o entidades privadas, deberá protegerse de acuerdo con la normativa aplicable.

Disposición adicional cuarta. *Seguridad de la información clasificada entregada a organismos ajenos al Ministerio de Defensa.*

1. La entrega de información clasificada del Ministerio de Defensa a organizaciones internacionales o países extranjeros se realizará al amparo de los convenios bilaterales o multilaterales en los que España sea parte.

2. La entrega de información clasificada del Ministerio de Defensa a otros órganos de las Administraciones Públicas, entidades privadas u organismos internacionales no gubernamentales se realizará de acuerdo con la normativa aplicable, conforme a los acuerdos y convenios establecidos.

Disposición adicional quinta. *Dependencia del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones.*

1. De acuerdo con lo establecido en la disposición adicional segunda del Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas, el Jefe de Estado Mayor de la Defensa ejercerá sobre el Centro de



Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) las competencias que le permitan ejercer su autoridad sobre la Infraestructura Integral de Información para la Defensa (I3D) en el ámbito operativo y la supervivencia de los servicios críticos para la defensa y las Fuerzas Armadas, con arreglo a lo establecido en los artículos 12.3.b) y 15.2 de la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

2. Las citadas competencias sobre todos los servicios críticos para la operatividad de la estructura operativa de las Fuerzas Armadas y de la Fuerza Conjunta serán ejercidas por el Jefe de Estado Mayor de la Defensa, a través de los Mandos de la estructura operativa que designe, cuando así lo considere.

Disposición adicional sexta. *Seguridad de la información en operaciones militares.*

Los Mandos de la estructura operativa y Mandos de Preparación de la Fuerza establecerán las medidas necesarias respecto a la seguridad de la Información de las operaciones, incluidas en el concepto más amplio de Seguridad Operacional (OPSEC), siguiendo las disposiciones emanadas de esta Política y del cuerpo normativo que la desarrolle.

Disposición transitoria única. *Vigencia temporal de las disposiciones derogadas.*

En tanto no se publiquen las nuevas disposiciones de «Aplicación de la política de seguridad de la información del Ministerio», «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información de las Empresas», correspondientes a las disposiciones elaboradas para la aplicación de esta norma, se mantendrá la vigencia de las disposiciones derogadas en la disposición derogatoria única, en todo aquello que no contravenga la presente orden ministerial.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada 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.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango, en aquello que se opongan a lo establecido en esta orden ministerial.

Disposición final primera. *Modificación de la 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 (CIS/TIC) del Ministerio de Defensa.*

La 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 queda redactada en los siguientes términos:

Uno. Artículo 7.2 letra b):

«Se establecerá una única arquitectura de referencia para la Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT) para la Infraestructura Integral de Información para la Defensa (I3D), que desarrollará el Mando Conjunto del Ciberespacio (MCCE), en coordinación con el CESTIC y los Ámbitos, considerando las medidas de seguridad definidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en la normativa relativa a la protección de datos de carácter personal, y en la normativa del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).»



Dos. Artículo 12.1 letra c):

«c) El Comité de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones del Ministerio de Defensa en relación al Plan de Acción de los Servicios de Seguridad de la Información. Este comité se fusiona con el Comité del Área de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (Comité SEGINFOSIT), regulado por la Política de Seguridad de la Información del Ministerio.»

Disposición final segunda. *Facultad de aplicación.*

Se faculta a la persona titular de la Secretaría de Estado de Defensa a dictar las disposiciones oportunas, en el ámbito de sus competencias, para la aplicación y ejecución de esta orden ministerial.

Disposición final tercera. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 22 de julio de 2024.–La Ministra de Defensa, Margarita Robles Fernández.

ANEXO

Política de seguridad de la información del Ministerio de Defensa

CAPÍTULO I

Disposiciones generales

Primero. *Objeto.*

El objeto de esta política es establecer las directrices, marco de actuación y estructura para alcanzar la protección adecuada, proporcionada y razonable de la información manejada por el Ministerio de Defensa, mediante la preservación de sus dimensiones de seguridad: confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad, así como la garantía de los derechos y libertades de las personas respecto a la protección de datos de carácter personal.

Segundo. *Ámbito de aplicación.*

Esta política es de aplicación a todo el Ministerio de Defensa y sus organismos autónomos.

A los efectos de aplicación de esta política, los ámbitos en el marco de la seguridad de la información del Ministerio de Defensa serán el Estado Mayor de la Defensa, la Secretaría de Estado de Defensa (que incluye las unidades y órganos con dependencia directa de la persona titular del Ministerio de Defensa, excepto el Centro Nacional de Inteligencia), la Subsecretaría de Defensa, la Secretaría General de Política de Defensa, el Ejército de Tierra, la Armada y el Ejército del Aire y del Espacio.

Al Centro Nacional de Inteligencia le será de aplicación únicamente los capítulos I, II y V en sus disposiciones decimonovena y vigésimo primera, sin perjuicio de las particularidades que procedan de acuerdo con su normativa específica.

Tercero. *Principios básicos y requisitos de la Seguridad de la Información.*

La información es un concepto abstracto e intangible que se obtiene, elabora, presenta, almacena, procesa, transporta o destruye (en adelante, maneja) mediante elementos tangibles. Estos elementos son: las personas, los documentos, los materiales,



los sistemas de información y telecomunicaciones, las instalaciones y las organizaciones. De acuerdo con ello, la protección de la información se realizará mediante la aplicación y supervisión de medidas de seguridad y procedimientos dirigidos a las personas, los datos de carácter personal, los documentos, los sistemas de información y telecomunicaciones, las instalaciones y las empresas.

Adicionalmente, en el caso concreto de la información tratada y los servicios prestados por medios electrónicos, se deberán cumplir los principios básicos y requisitos de seguridad de la información recogidos en el Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022, de 3 de mayo.

CAPÍTULO II

Protección de la información

Cuarto. *Conceptos generales.*

Se consideran «materias clasificadas» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado. Estas «materias clasificadas» serán exclusivamente las que, de acuerdo con la Ley 9/68, de 5 de abril, sobre secretos oficiales, se definen como Secreto y Reservado en el apartado, «Grados de clasificación de la información».

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. Estas materias son las que posteriormente se definen como Confidencial y Difusión Limitada en el apartado quinto, «Grados de clasificación de la información».

A efectos de la presente política, las «materias clasificadas» y las «materias objeto de reserva interna» quedan englobadas en el concepto general de «información clasificada».

La persona titular de la Secretaría de Estado de Defensa aprobará la disposición que establezca la aplicación de todos los procesos de clasificación de la información.

Quinto. *Grados de Clasificación de la Información.*

1. Los grados de clasificación de la información son:

– Secreto (S): se aplicará a la información que precise del más alto nivel de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgo, amenaza o perjuicio extremadamente grave de la seguridad y defensa del Estado, así como comprometer los intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.

– Reservado (R): se aplicará a la información no comprendida en el apartado anterior pero cuyo conocimiento o divulgación no autorizados pudiera afectar a los referidos intereses fundamentales de la Nación, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

– Confidencial (C): se aplicará a la información no comprendida en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, amenazar o perjudicar sus intereses o dificultar el cumplimiento de su misión.

– Difusión Limitada (DL): se aplicará a la información no comprendida en los apartados anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

2. Autoridades y órganos facultados para clasificar.

– La facultad para clasificar la información de grado Secreto o Reservado corresponde al Consejo de Ministros.



– La facultad para clasificar la información de grado Confidencial o Difusión Limitada corresponde, en el ámbito de su competencia, a las siguientes autoridades:

Persona titular del Ministerio de Defensa.
Jefe de Estado Mayor de la Defensa.
Persona titular de la Secretaría de Estado de Defensa.
Persona titular de la Dirección del CNI.
Persona titular de la Subsecretaría de Defensa.
Jefe de Estado Mayor del Ejército.
Almirante Jefe de Estado Mayor de la Armada.
Jefe de Estado Mayor del Ejército del Aire y del Espacio.
Persona titular de la Secretaría General de Política de Defensa.

Estas autoridades podrán delegar oficialmente dicha atribución.

Sexto. *Información No Clasificada.*

Atendiendo a su ámbito de distribución, la información no clasificada podrá ser:

– Información de Uso Oficial: información cuya distribución está limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el departamento.

– Información de Uso Público: información cuya distribución no está limitada al ámbito del Ministerio de Defensa, o personas y organismos que desempeñen actividades relacionadas con el departamento.

– Información Sensible: cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, con independencia de que se le haya asignado o no una clasificación de seguridad.

Se establecerán los procedimientos para proteger la información sensible, así definida por su propietario, ya que su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o algo. La persona titular de la Secretaría de Estado de Defensa aprobará la disposición que regule estos aspectos transversales a las diferentes áreas.

CAPÍTULO III

Protección de datos de carácter personal

Séptimo. *Protección de datos de carácter personal.*

1. Toda información que contenga datos de carácter personal, tratada por el Ministerio de Defensa y sus organismos vinculados o dependientes, ya sean tratamientos automatizados o no automatizados, se ajustará a lo exigido por el 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, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y al resto de la normativa aplicable.

2. Cuando se traten datos personales, será de aplicación lo dispuesto en la normativa de protección de datos, así como los criterios que se establezcan por la Agencia Española de Protección de Datos.

3. El tratamiento de datos de carácter personal se efectuará conforme a los principios de licitud, transparencia y lealtad, finalidad, minimización, exactitud, limitación del plazo de conservación y seguridad.

4. De acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la normativa en

materia de protección de datos de carácter personal no será de aplicación a los tratamientos que tengan la consideración de materias clasificadas de acuerdo con lo establecido en esta política.

CAPÍTULO IV

Áreas de seguridad de la información del Ministerio de Defensa

Octavo. *Áreas de Seguridad de la Información.*

La seguridad de la información se estructura funcionalmente en áreas, para permitir la dirección, aplicación, ejecución, apoyo y auditoría de medidas de protección homogéneas. Las áreas funcionales, atendiendo a su finalidad son:

- Seguridad de la Información en las Personas.
- Seguridad de la Información de los datos de Carácter Personal.
- Seguridad de la Información en los Documentos.
- Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.
- Seguridad de la Información en las Instalaciones.
- Seguridad de la Información en poder de las Empresas.

a) Seguridad de la Información en las Personas (SEGINFOPER).

Conjunto de medidas y los procedimientos establecidos para reducir, a un grado mínimo aceptable, cualquier comprometimiento de la información por causa exclusivamente del personal que accede a ella, sea voluntaria o involuntariamente, o de forma autorizada o no.

b) Seguridad de la Información de los datos de Carácter Personal (SEGINFOCAP).

Medidas técnicas y organizativas dirigidas a garantizar el derecho fundamental de las personas físicas a la protección de sus datos personales, así como la protección de la confidencialidad de la información que contenga datos de carácter personal manejada por el Ministerio de Defensa en cualquiera de sus actividades, garantizando los derechos y libertades de los interesados, de acuerdo con lo previsto en la normativa aplicable vigente en cada momento.

c) Seguridad de la Información en los Documentos (SEGINFODOC).

Medidas de seguridad de la información orientadas a disuadir, prevenir y detectar los incidentes de seguridad de la información en los documentos, excluyendo aquellos que se encuentren dentro de los sistemas de información y telecomunicaciones, y, en caso de incidente, minimizar los daños y adoptar las medidas adecuadas para evitar su repetición.

d) Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT).

Medidas y procedimientos diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información manejada mediante sistemas y servicios de tecnologías de la información y las comunicaciones (CIS/TIC), así como su trazabilidad y autenticidad.

e) Seguridad de la Información en las Instalaciones (SEGINFOINS).

Medidas de protección eficaz para la prevención de posibles accesos a información por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.

La seguridad deberá ser concebida de forma global, mediante una combinación de medidas físicas complementarias que garanticen un grado de protección suficiente, coordinando su aplicación con el resto de medidas de seguridad.



f) Seguridad de la Información en poder de las Empresas (SEGINFOEMP).

Medidas de seguridad establecidas para proteger la información del Ministerio de Defensa en poder de las empresas, con el objeto de que se garantice razonablemente la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de la información del departamento manejada por éstas, como consecuencia de su participación en programas, proyectos o contratos del Ministerio de Defensa.

CAPÍTULO V

Estructura organizativaNoveno. *Niveles funcionales.*

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:

- Nivel departamental, que afecta a todo el Ministerio de Defensa.
- Nivel específico, que afecta a cada uno de los Ámbitos el Ministerio de Defensa.

*Sección 1.ª Nivel departamental*Décimo. *Director de Seguridad de la Información del Ministerio de Defensa.*

1. El Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF), realiza las funciones establecidas en el artículo 2 de esta orden ministerial.

2. Una Instrucción de la Secretaría de Estado de Defensa detallará los cometidos que se le atribuyen. En tanto se publica ésta, asumirá los cometidos de «Autoridad Delegada de Acreditación» (ADA) que, en el ámbito de los Sistemas responsabilidad del Órgano Central y periféricos del Ministerio de Defensa, asignaba al Subsecretario de Defensa el Título Cuarto de la Orden Ministerial 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.

Undécimo. *Subdirector de Seguridad de la Información del Ministerio de Defensa.*

1. Se designa como Subdirector de Seguridad de la Información del Ministerio de Defensa (SDSIDEF) a la persona titular de la Dirección General del CESTIC. Tiene como cometidos la asistencia y apoyo al DSIDEF en la dirección, impulso y gestión de la política de seguridad de la información del Ministerio de Defensa, así como en la definición y creación de la estructura funcional de la seguridad de la información, incluyendo en esta última el Servicio de Protección de Materias Clasificadas.

2. La persona titular de la Secretaría de Estado de Defensa detallará, mediante instrucción, los cometidos que se le atribuyen.

Duodécimo. *Responsables de las áreas de seguridad de la información-RAS.*

1. Los responsables de las áreas de seguridad de la información coordinarán y supervisarán la seguridad de la información en sus respectivas áreas.

2. La persona titular de la Secretaría de Estado de Defensa detallará, mediante instrucción, la asignación de la titularidad de cada uno de los responsables, así como los cometidos que se le atribuyen.

*Sección 2.^a Nivel específico**Decimotercero. Responsable de seguridad de la información-RSI.*

1. En cada uno de los Ámbitos habrá un Responsable de Seguridad de la Información, nombrado por la Autoridad del Ámbito, que dirigirá y coordinará las medidas de seguridad de la información en todas las áreas de seguridad de la información de su ámbito.

2. La persona titular de la Secretaría de Estado de Defensa detallará, mediante instrucción, los cometidos que se le atribuyen.

Decimocuarto. Jefe de seguridad de la información-JSI.

1. En cada uno de los ámbitos habrá un jefe de seguridad de la información, nombrado por la autoridad del ámbito respectivo, a propuesta del responsable de seguridad de la información correspondiente; tendrá rango mínimo de jefe de área, coronel o capitán de navío.

2. Será responsable de la ejecución y supervisión de las medidas de seguridad de la información en todas las áreas de seguridad de la información de su ámbito.

3. La persona titular de la Secretaría de Estado de Defensa detallará, mediante instrucción, los cometidos que se le atribuyen.

Decimoquinto. Jefes de las áreas de seguridad de la información de su ámbito-JAS.

1. El responsable de seguridad de la información organizará en su ámbito las áreas de seguridad. Designará a los jefes en las diversas áreas, que dependerán funcionalmente del Jefe de Seguridad de la Información de su ámbito y serán responsables de los cometidos que éste les encomiende en relación con su respectiva área de seguridad de la información.

2. La persona titular de la Secretaría de Estado de Defensa detallará, mediante instrucción, los cometidos que se les atribuyen.

*Sección 3.^a Protección de Datos de Carácter Personal**Decimosexto. Estructura de Protección de Datos de Carácter Personal.*

1. Para el ejercicio de las funciones establecidas en materia de protección de datos de carácter personal, se establece la estructura compuesta por las figuras de Responsable de Tratamiento y Delegado de Protección de Datos, y los órganos siguientes:

- Oficina Central de Protección de Datos de Carácter Personal (OCCAP).
- Oficina Específica de Protección de Datos de Carácter Personal del Ámbito (OECAP).

2. La persona titular de la Secretaría de Estado de Defensa establecerá el funcionamiento de esta estructura.

*Sección 4.^a Servicio de Protección de Materias Clasificadas**Decimoséptimo. Estructura del Servicio de Protección de Materias Clasificadas.*

1. El Servicio de Protección de Materias Clasificadas (SPMC) del Ministerio de Defensa está compuesto por los siguientes órganos, denominados genéricamente órganos de control:

- El Servicio Central de Protección de Materias Clasificadas (SCPMC).
- Los Servicios Generales de Protección de Materias Clasificadas (SGPMC).
- Los Servicios Locales de Protección de Materias Clasificadas (SLPMC).



2. El SPMC 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.

3. La persona titular de la Secretaría de Estado de Defensa establecerá la estructura de este servicio.

Sección 5.^a Servicio de Gestión y Control de Material de Cifra en el Ministerio de Defensa

Decimoctavo. *Estructura de gestión y control del material de cifra en el Ministerio de Defensa.*

La estructura de gestión y control del material de cifra en el ámbito del Ministerio de Defensa se organiza en los siguientes términos:

a) Estructura de gestión y control del material de cifra nacional compuesta de los siguientes órganos:

- Órgano de Control de Material de Cifra (OCMC).
- Órganos de Distribución de Material de Cifra (ODMC).
- Órganos de Distribución de Material de Cifra Secundarios (ODMCS).

Esta estructura nacional estará dirigida y regulada por la Autoridad de Control de Material de Cifra (ACMC), que velará por la correcta gestión y control del material de cifra nacional del departamento.

También existirá una Autoridad de Control Delegada (ACMC-D), que asumirá aquellos cometidos que determine la ACMC.

El OCMC actuará como órgano de apoyo técnico de la ACMC / ACMC-D.

b) Estructura de gestión y control del material de cifra no nacional compuesta de los siguientes órganos:

- Agencia Nacional de Distribución de Material de Cifra (ESP NDA), constituida como cuenta de cifra principal OTAN/UE/ESA a nivel nacional.
- Subcuentas de cifra OTAN/UE/ESA, constituidas en el ámbito corporativo del MDEF, dependientes de la ESP NDA.

Sección 6.^a Esquema Nacional de Seguridad

Decimonoveno. *Estructura de adecuación al Esquema Nacional de Seguridad.*

Para adecuar los Sistemas de Información y Telecomunicaciones del Ministerio de Defensa al Esquema Nacional de Seguridad, se designarán los responsables de cada Sistema, cuyos cometidos, alcance y proceso de nombramiento se detallarán en normas del nivel adecuado, de acuerdo con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

a) Responsable funcional, que integra la figura del responsable de la información y del responsable del servicio y determinará los requisitos de la información tratada y de los servicios prestados.

b) Responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo.

Podrá designar motivadamente, siendo responsable de su actuación, los responsables de seguridad delegados que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con



sus criterios. Para los sistemas ajenos a la I3D, el RSI del ámbito al que pertenezca el sistema nombrará al responsable de seguridad.

c) Responsable del sistema, que tiene la responsabilidad de desarrollar, operar y mantener el sistema de información que soporta los distintos servicios, durante todo su ciclo de vida. Podrá designar motivadamente, siendo responsable de su actuación, los responsables de sistema delegados que consideren necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios. Para los sistemas ajenos a la I3D, el RSI del ámbito al que pertenezca el sistema, nombrará al responsable del sistema.

CAPÍTULO VI

Gobernanza de la seguridad de la información del Ministerio de Defensa

Vigésimo. *Gobernanza.*

1. La estructura de gobernanza desarrollará sus funciones en los aspectos esenciales de la seguridad de la información del Ministerio de Defensa, incluyendo, entre otros, la cooperación dentro del departamento y con otros organismos nacionales e internacionales, el desarrollo de la normativa necesaria, la gestión de riesgos, la auditoría de seguridad y certificación de conformidad, la concienciación y formación, los aspectos relativos a la gestión de incidentes, ciberincidentes y brechas de seguridad y la monitorización y vigilancia de la seguridad de la información, entre otros. Estos procesos se desarrollarán en la normativa correspondiente, en la cual se designarán los responsables de cada uno.

2. Para el correcto funcionamiento de la estructura de gobernanza y la adecuada orientación de sus funciones, es necesario que quienes la componen mantengan el conocimiento preciso de la situación de seguridad de la información del departamento y en especial, del ciberespacio. En consecuencia, la estructura de gobernanza de la seguridad de la información del Ministerio de Defensa, y las operaciones militares que las Fuerzas Armadas lleven a cabo en el ciberespacio deben compartir la necesaria conciencia situacional, para resolver los problemas de seguridad de la información que surjan.

3. La persona titular de la Secretaría de Estado de Defensa establecerá la estructura de gobierno y sus funciones, detallando las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Vigésimo primero. *Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.*

El Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa (CDSIDDEF) es el órgano de coordinación y seguimiento de la política de seguridad de la información del Ministerio de Defensa. Su composición es la siguiente:

Presidente: la persona titular de la Secretaría de Estado de Defensa.

Vocales:

El Secretario General del CNI.

El Jefe de Estado Mayor Conjunto de la Defensa.

El Segundo Jefe de Estado Mayor del Ejército.

El Segundo Jefe de Estado Mayor de la Armada.

El Segundo Jefe del Estado Mayor del Ejército del Aire y del Espacio.

El Secretario General Técnico.

El Director General de Política de Defensa.

Secretario y vocal: el Director General del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones.



Asesores, con voz, pero sin voto:

- El Director General de Armamento y Material.
- El Director General de Personal.
- El Director General de Infraestructura.
- El Comandante del Mando Conjunto del Ciberespacio.
- El Delegado de Protección de Datos del Ministerio de Defensa.

Vigésimo segundo. *Estructura de la Comisión Ejecutiva de la Seguridad de la Información del Ministerio de Defensa.*

Bajo la dirección e indicaciones del CDSIDEF, se establece una Comisión Ejecutiva (CESIDEF), responsable de la coordinación, seguimiento y control del desarrollo de la presente Política, a través del Plan de Actuación.

La CESIDEF estará compuesta por los siguientes miembros:

- Presidente: la persona titular de la Dirección General del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones.
- Vocales: los jefes de seguridad de la información (JSI) de los ámbitos y los responsables de cada una de las áreas de seguridad de la información o personal específicamente designado por éstos.
- 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.

El delegado de Protección de Datos asistirá en calidad de asesor.

Vigésimo tercero. *Estructura de los comités de la seguridad de la información del Ministerio de Defensa.*

1. Se establecen los comités de la seguridad de la información del Ministerio de Defensa para el seguimiento y control de los Planes de Acción de las áreas de seguridad de la información. Existirá un comité por cada una de las áreas de seguridad de la información descritas en la disposición octava.

2. Cada comité de seguridad de la información de un área determinada estará compuesto por los siguientes miembros:

- Presidente: el responsable del área de seguridad de la información correspondiente.
- Vocales: los Jefes de las áreas de seguridad de la información (JAS) de los Ámbitos del nivel específico.
- Secretario: un oficial de empleo coronel, capitán de navío o funcionario de nivel 29, designado por el presidente del Comité.

CAPÍTULO VII

Otras disposiciones

Vigésimo cuarto. *Ejecución dispositiva de la política de seguridad de la información.*

1. Mediante una disposición se desarrollará este anexo sobre seguridad de la información, enmarcando cada conjunto de normas en distintos niveles por amplitud del aspecto tratado y ámbito de aplicación.

2. Aquellas disposiciones de carácter operativo que afecten a las actividades de preparación de las Fuerzas Armadas o las operaciones militares y que afecten a la seguridad operacional, incluida la seguridad de la información, deberán ser aprobadas por el Jefe de Estado Mayor de la Defensa o los Mandos de la estructura operativa que éste designe, cuando así lo considere.



3. Cada disposición de un nivel determinado debe fundamentarse en las de nivel superior.

a) Primer nivel.

Una única disposición que establece principios generales abarcando todo el ámbito de la seguridad de la información. Está constituido por el presente documento de «política de seguridad de la información del Ministerio de Defensa».

b) Segundo nivel.

Conjunto de disposiciones que desarrollan y detallan la presente política, abarcando un área, sub-área o aspecto determinado de la seguridad de la información. Su ámbito de aplicación será todo el departamento.

El desarrollo de este segundo nivel de la seguridad de la información incluirá, al menos, las siguientes instrucciones y planes:

- Aplicación de la política de seguridad de la información del Ministerio de Defensa.
- Seguridad de la Información en las Personas.
- Seguridad de la Información en Protección de Datos de Carácter Personal.
- Seguridad de la Información en los Documentos.
- Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.
- Seguridad de la Información en las Instalaciones.
- Seguridad de la Información en poder de las Empresas.
- Plan de Actuación departamental.
- Normas de elaboración, clasificación, cesión, distribución y destrucción de la información.
- Estructura de Protección de Datos de Carácter Personal.
- Estructura del Servicio de Protección de Materias Clasificadas.
- Estructura funcional para la gestión y control de material de cifra nacional del Ministerio de Defensa.

c) Tercer nivel normativo.

Conjunto de disposiciones que desarrollan y detallan la disposición de segundo nivel. Está constituido por normas de carácter eminentemente técnico y procedimental. Dependiendo del aspecto tratado, podrá ser de aplicación a todo el departamento, un ámbito específico o un sistema determinado.

Cada disposición se aprobará en el nivel inmediatamente superior al que la elabora. La persona titular del departamento aprobará las de primer nivel; el CDSIDEF hará lo propio con las de segundo nivel y la CESIDEF aprobará la normativa de tercer nivel.



V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

ZONAS DE INTERÉS PARA LA DEFENSA NACIONAL

Cód. Informático: 2024018273. (Del BOE núm. 184, de 31-7-2024) (B. 152-4)

Real Decreto 835/2024, de 30 de julio, por el que se declara zona de interés para la Defensa Nacional la propiedad denominada «Campus Principal del Centro Tecnológico de Desarrollo y Experimentación», localizada en el término municipal de Jaén.

La función de Defensa Nacional es contenido esencial de la función política de Gobierno, y así lo expresa la Constitución en su artículo 149.1.4.º, al atribuir al Estado la competencia exclusiva de su defensa y al asignar al Gobierno la dirección de esta función en el artículo 97.

Compete, así, constitucionalmente al Gobierno dirigir la Política de Defensa y la Política Militar y adoptar, en su consecuencia, las condiciones necesarias para su mejor eficacia.

Esta eficacia viene recabando desde tiempo atrás, y hoy con mayor motivo y con carácter ineludible, disponer sin perturbaciones de un Centro de excelencia de I+D+i en los ámbitos de la defensa y la seguridad, para que mediante el desarrollo y experimentación de tecnologías avanzadas se dé adecuada respuesta y soporte a las nuevas capacidades militares requeridas para hacer frente a los riesgos y amenazas que se han puesto de manifiesto en recientes conflictos.

De este modo, la incorporación de soluciones tecnológicas innovadoras a las capacidades de las Fuerzas Armadas contribuirá de manera determinante al cumplimiento de las misiones que les son asignadas en el artículo 15 de la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

Igualmente, el artículo 30 de dicha ley orgánica prevé expresamente que en las zonas de territorio nacional consideradas de interés para la defensa podrá limitarse los derechos de nacionales y extranjeros de acuerdo con lo que se determine por ley.

Con este propósito, y con el fin de preservar la propiedad y sus instalaciones de cualquier actuación que pudiera afectarla, han sido adecuadamente ponderados los distintos intereses que pueden incidir en la zona que se declara de interés para la Defensa Nacional y que se extiende, en este caso, a la zona ocupada por el denominado «Campus Principal del Centro Tecnológico de Desarrollo y Experimentación» (CETEDEX), en el término municipal de Jaén, comprendiendo los límites de la propiedad dentro de las coordenadas que se detallan en el anexo a este real decreto, así como el espacio aéreo correspondiente a dicha extensión de terreno.

La denominación de zonas de interés para la Defensa Nacional viene recogida en el artículo 2 de la Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional, y en el artículo 2 del Reglamento de ejecución de la Ley 8/1975, aprobado por Real Decreto 689/1978, de 10 de febrero, mientras que la declaración de dichas zonas se llevará a cabo mediante la promulgación de un real decreto aprobado por el Consejo de Ministros, de acuerdo con el artículo 5 de esta misma ley, así como el artículo 5 de su Reglamento de ejecución.

La Comisión Interministerial de Defensa, que actúa por delegación del Consejo de Defensa Nacional, adoptó el día 22 de julio de 2024 el acuerdo de aprobar la propuesta de declaración de zona de interés para la Defensa Nacional de la propiedad denominada «Campus Principal del Centro Tecnológico de Desarrollo y Experimentación» (CETEDEX).



En su virtud, a propuesta de la Ministra de Defensa, y previa deliberación del Consejo de Ministros en su reunión del día 30 de julio de 2024,

DISPONGO:

Artículo 1. Declaración de zona de interés para la Defensa Nacional.

1. Se declara zona de interés para la Defensa Nacional la extensión de terreno comprendida en las coordenadas que se detallan en el anexo a este real decreto, en la que se encuentra la propiedad denominada «Campus Principal del Centro Tecnológico de Desarrollo y Experimentación» (CETEDEX), así como el espacio aéreo correspondiente a dicha extensión de terreno, localizada en el término municipal de Jaén.

2. En dicha zona se considerarán prioritarios los intereses de la Defensa Nacional, quedando bajo la responsabilidad y vigilancia del Instituto Nacional de Técnica Aeroespacial «Esteban Terradas», de acuerdo con lo previsto en el artículo 6 del Reglamento de ejecución de la Ley 8/1975, de 12 de marzo.

Artículo 2. Limitaciones y condicionantes.

Las limitaciones y condiciones que, conforme a lo establecido en el artículo 5 de la Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional, se imponen en la zona declarada de interés para la Defensa, son las siguientes:

a) Interesar y obtener autorización del Ministerio de Defensa para la determinación de la compatibilidad con los fines de la Defensa Nacional de cualquier regulación, ordenación o actuación administrativa que pueda incidir en la utilización militar de la extensión de terreno delimitada por las coordenadas reflejadas en el anexo y que comprenden a la propiedad denominada «Campus Principal del Centro Tecnológico de Desarrollo y Experimentación» (CETEDEX).

b) Someter a la autorización previa del Ministerio de Defensa la transmisión de la propiedad, así como la constitución, transmisión y modificación de cualquier derecho real sobre la misma, con independencia de la nacionalidad o naturaleza de los otorgantes.

c) Someter a la autorización previa del Ministerio de Defensa cualquier obra de edificación o construcción, promovida por entidades públicas o privadas, así como la cesión por cualquier título de los aprovechamientos agrícolas, pecuarios o cinegéticos de los territorios afectados.

d) Someter a la autorización previa del Ministerio de Defensa cualquier tipo de vuelo de aeronaves pilotadas por control remoto, en espacio aéreo declarado de interés para la Defensa Nacional.

Disposición final primera. Título competencial.

Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.4.^a de la Constitución, que atribuye al Estado la competencia exclusiva sobre Defensa y Fuerzas Armadas.



Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Palma, el 30 de julio de 2024.

FELIPE R.

La Ministra de Defensa,
MARGARITA ROBLES FERNÁNDEZ



ANEXO

El anexo se puede consultar de manera íntegra en el siguiente enlace a la página web del INTA:

https://www.inta.es/export/sites/default/galleries/Galeria-pdfs-de-paginas/ANEXO-zona-de-interes-para-la-Defensa-CETEDEX_v2.pdf

**V. — OTRAS DISPOSICIONES****MINISTERIO DE HACIENDA****SECTOR PÚBLICO ESTATAL. CUENTAS ANUALES**

Cód. Informático: 2024018274. (Del BOE núm. 184, de 31-7-2024) (B. 152-5)

Resolución de 22 de julio de 2024, de la Intervención General de la Administración del Estado, por la que se publica la referencia al «Registro de cuentas anuales del sector público» del ejercicio 2023.

<https://www.boe.es/boe/dias/2024/07/31/pdfs/BOE-A-2024-15836.pdf>