BOD

BOLETÍN OFICIAL DEL MINISTERIO DE DEFENSA

AÑO XXXV • VIERNES, 3 DE MAYO DE 2019 • NÚMERO 86

SUMARIO

I. — DISPOSICIONES GENERALES

III. — PERSONAL

CVE: BOD-2019-s-086-295
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

IV. — ENSEÑANZA MILITAR

RETRIBUCIONES

CVE: BOD-2019-s-086-296
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

ARMADA

Edita:

MINISTERIO DE DEFENSA SECRETARÍA GENERAL TÉCNICA

Diseño y Maquetación:
Imprenta del Ministerio de Defensa

CVE: BOD-2019-s-086-297
Verificable en https://sede.defensa.gob.es/acceda/bod

I. — DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

CIBERSEGURIDAD

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia Nacional de Ciberseguridad 2019.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

Madrid, 26 de abril de 2019.–La Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, Carmen Calvo Poyato.

ANEXO

Estrategia Nacional de Ciberseguridad 2019

Sumario

CVE: BOD-2019-086-11349
Verificable en https://sede.defensa.gob.es/acceda/bod

Resumen ejecutivo

La Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

El documento se estructura en cinco capítulos. El primero, titulado «El ciberespacio, más allá de un espacio común global», proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio una de los principales riesgos para nuestro desarrollo como nación.

Por ello, la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

Contribuir a la promoción de un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podemos enfrentar, incluyendo nuevas y emergentes.

El segundo capítulo, titulado «Las amenazas y desafíos en el ciberespacio» determina las principales amenazas del ciberespacio que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

El tercer capítulo, titulado «Propósito, principios y objetivos para la ciberseguridad» aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos. Su desarrollo, se plasma en el cuarto capítulo titulado «Líneas de acción y medidas», donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio; impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el

CVE: BOD-2019-086-11350
Verificable en https://sede.defensa.gob.es/acceda/bod

ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El quinto capítulo, titulado «La ciberseguridad en el Sistema de Seguridad Nacional» define la arquitectura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el foro Nacional de Ciberseguridad.

Asimismo, en este último capítulo, se exponen a modo de conclusión, unas consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la Estrategia.

Introducción

La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. El documento fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone, para el país, la vulnerabilidad del ciberespacio. Además, la estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional. Igualmente, en estos años, España ha seguido avanzando en sus esfuerzos por contribuir a la promoción de un ciberespacio seguro y fiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional. Desde su primera reunión, el Consejo Nacional de Ciberseguridad ha asumido la tarea de coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad y sus planes derivados. Así, hoy España cuenta con organismos especializados en ciberseguridad y una posición destacada a nivel europeo e internacional.

El marco jurídico también ha experimentado una notable adaptación. En respuesta a su evolución y a la experiencia acumulada en estos años, en 2015 se publicó la modificación del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del Sector Público. Por otro lado, la entrada en vigor del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS), ha supuesto un importante hito en la mejora de la ciberseguridad en nuestro país, extendiendo el alcance de esta Directiva con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional se promulgó con vocación de dar impulso a uno de los proyectos de mayor responsabilidad para un

CVE: BOD-2019-086-11351
Verificable en https://sede.defensa.gob.es/acceda/bod

gobierno, la Seguridad Nacional. La Ley de Seguridad Nacional contempla la ciberseguridad como ámbito de especial interés.

Se puede afirmar, sin lugar a dudas, que la ciberseguridad ha modernizado la Seguridad Nacional, tratándose de uno de los ámbitos de mayor avance hasta la fecha. Esta dinámica debe seguir su camino adelante.

La Estrategia de Seguridad Nacional 2017 marca un punto de inflexión en el pensamiento estratégico nacional, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

Ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, y para el que la colaboración público-privada es un elemento clave, resulta necesaria una nueva aproximación, una nueva estrategia nacional de ciberseguridad.

CAPÍTULO 1

El ciberespacio como espacio común global

Este capítulo presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter inherentemente internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

El ciberespacio: oportunidades y desafíos:

El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

Por una parte, el ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Se constituye así en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. La inteligencia artificial, la robótica, el big data, el blockchain y el internet de las cosas son ya una realidad, si bien el verdadero potencial transformador está todavía por descubrir. Sus implicaciones van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

Por otra parte, la digitalización transforma la seguridad y presenta serios desafíos. El ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica,

CVE: BOD-2019-086-11352
Verificable en https://sede.defensa.gob.es/acceda/bod

reordenación del poder y empoderamiento del individuo. Así, la creciente conectividad y la mayor dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales, generan vulnerabilidades y dificultan la adecuada protección de la información.

Infraestructura digital:

Además de su naturaleza virtual, el ciberespacio se sustenta en elementos físicos y lógicos. Los dispositivos, componentes y sistemas que constituyen las redes y sistemas de información y comunicaciones están expuestos a disfunciones que alteran su correcto funcionamiento y a acciones deliberadas con fines malintencionados, que ponen en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas.

Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

Todos estos elementos, unidos a la creciente interconectividad entre sistemas pueden originar efectos en cascada con resultados impredecibles.

Plano internacional: seguridad en el ciberespacio:

La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza. En este contexto, España defiende su visión e intereses como nación y contribuye al esfuerzo conjunto de la comunidad internacional en su apuesta por un ciberespacio abierto, plural y seguro.

España continúa participando activamente en todas las instituciones en las que la ciberseguridad ocupa un lugar destacado, en especial en el marco de la Unión Europea, la Alianza Atlántica y de Naciones Unidas, demostrando así el compromiso con sus socios y aliados. Asimismo, se mantienen vínculos con terceros Estados mediante mecanismos de cooperación bilateral que facilitan elementos de entendimiento y confianza mutua basados en las relaciones fluidas en el ámbito de la ciberseguridad y orientados hacia la construcción de capacidades.

Consciente de la importancia del multilateralismo, además del Derecho Internacional y las normas no vinculantes de comportamiento responsable de los Estados, se destaca el papel de La Carta de Naciones Unidas como principio de referencia para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio. La construcción de consensos y las medidas de fomento de confianza constituyen la base para su aplicación y puesta en práctica, así como los Tratados y Convenios Internacionales en los que España es parte.

Una nueva concepción del ciberespacio:

Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.

El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado.

En primer lugar, el sector privado juega un papel relevante como uno de los gestores y propietarios de los activos digitales de España, por lo que las capacidades de ciberseguridad del país residen en gran medida en las de sus empresas. Es por tanto necesario el apoyo, la promoción y la inversión en ciberseguridad para impulsar la

CVE: BOD-2019-086-11353
Verificable en https://sede.defensa.gob.es/acceda/bod

competitividad y el crecimiento económico, a la vez que proporcionar un entorno digital seguro y fiable.

Por otra parte, se debe aspirar a incrementar la autonomía tecnológica mediante el fomento de una base industrial nacional de ciberseguridad, la I+D+i y la gestión del talento tecnológico. En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento o de formación requerida.

En segundo lugar, la transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore elementos de mayor fuerza disuasoria obedece a un contexto global de mayor competencia geopolítica. El empleo del ciberespacio como dominio de confrontación, de forma independiente o como parte de una acción híbrida, es un rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.

En tercer lugar, la rápida evolución de las ciberamenazas aconseja una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones. Así mismo, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución.

A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.

CAPÍTULO 2

Las amenazas y desafíos en el ciberespacio

En este capítulo se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España.

La promoción de un entorno seguro y fiable es una tarea que debe partir del conocimiento y la comprensión de los desafíos y las amenazas, incluyendo las nuevas y emergentes que afectan al ciberespacio. La Estrategia de Seguridad Nacional de 2017 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

Ciberamenazas:

Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

Su carácter transversal, exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

En este escenario, las defensas deben evolucionar continuamente para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto

CVE: BOD-2019-086-11354
Verificable en https://sede.defensa.gob.es/acceda/bod

llamada que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

En este sentido, la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Acciones que usan el ciberespacio para fines maliciosos:

Las tecnologías digitales dan entrada a nuevas actividades y formas de negocio que requieren ser debidamente reguladas, pues pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Igualmente, las mismas cualidades que hacen del ciberespacio un motor del progreso, pueden ser explotadas con fines perniciosos al sumarse a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación.

Debido a la revolución de Internet, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable en otros tiempos. La conectividad digital lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada.

Las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas incluyen las relacionadas con el ciberespionaje y la cibercriminalidad.

El ciberespionaje es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional, dada la dificultad de atribución de la autoría. Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas (APT). Un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción para ejecutar sus objetivos.

Asimismo, se constata una tendencia creciente de las denominadas amenazas híbridas, acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.

La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término Cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una

CVE: BOD-2019-086-11355
Verificable en https://sede.defensa.gob.es/acceda/bod

fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos.

CAPÍTULO 3

Propósito, principios y objetivos para la ciberseguridad

En este capítulo se establece el propósito y los principios por los que se rige la Estrategia, así como los objetivos: uno general y cinco específicos.

Propósito:

España precisa, tal y como establece la Estrategia de Seguridad Nacional de 2017, garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable.

Por tanto, el propósito de la Estrategia Nacional de Ciberseguridad 2019, es fijar las directrices generales del ámbito de la ciberseguridad de manera que se alcancen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

Para ello, España ha de seguir avanzando en el refuerzo de capacidades para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio. En consecuencia, se seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

CVE: BOD-2019-086-11356
Verificable en https://sede.defensa.gob.es/acceda/bod

Por otra parte, el fomento de la cultura de ciberseguridad ha de ser uno de los ejes centrales a desarrollar a fin de contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida.

Asimismo, la ciberseguridad es progreso, por lo que el apoyo e impulso de la industria española de ciberseguridad, la promoción de un entorno que favorezca la investigación, el desarrollo y la innovación, y la participación del mundo académico tiene un carácter singular. Por otro lado, es un objetivo prioritario en nuestra sociedad alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas y profesionales, ya que solo mediante su promoción se podrá responder a los grandes retos de la ciberseguridad.

La transversalidad y globalidad del ciberespacio, requiere además de la cooperación y del cumplimiento del Derecho internacional, del máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas; en coherencia con la Estrategia de Seguridad Nacional y con las iniciativas desarrolladas en el marco europeo, regional e internacional, prevaleciendo en todo momento los intereses nacionales.

Principios rectores:

La Estrategia Nacional de Ciberseguridad, se sustenta y se inspira en los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia.

Unidad de Acción: Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

Una gestión centralizada de las crisis que afecten al ciberespacio, permite mantener una visión completa de la situación de la amenaza y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

Anticipación: La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente deber participar el sector privado.

La anticipación prima las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, con información compartida lo más próximo al tiempo real, permite alcanzar un adecuado conocimiento de la situación. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas.

Eficiencia: La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación. A lo anterior se suma la necesidad de una planificación anticipada y una elevada complejidad en su sostenimiento.

Además, el escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los dedicados a la ciberseguridad, por lo que resultarán indispensables la unidad de acción, compartición de información e integración de estos recursos para alcanzar la eficiencia deseada.

Resiliencia: La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas. Especial mención merece el refuerzo que requieren las redes de información y comunicaciones frente a actividades de las ciberamenazas o al uso ilícito del ciberespacio.

CVE: BOD-2019-086-11357
Verificable en https://sede.defensa.gob.es/acceda/bod

Objetivo general:

Los nuevos retos de la ciberseguridad han requerido la adaptación de su objetivo general de manera que se muestre más integrador, inclusivo y menos tecnificado.

En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Basados en este objetivo general, a continuación, se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito.

Objetivo I

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

Es necesario consolidar un marco nacional coherente e integrado que ayude a garantizar la protección de la información manejada por el sector público y por los servicios esenciales, sus sistemas y servicios, así como de las redes que los soportan. Este marco permitirá desarrollar e implantar servicios cada vez más seguros y eficientes.

Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

En particular, las acciones contra el ciberespionaje merecen especial mención para asegurar la protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

El sector público y los operadores de servicios esenciales se deben involucrar activamente en un proceso de mejora continua respecto de la protección de sus sistemas de Tecnologías de la Información y las Comunicaciones basados en una vigilancia permanente de su exposición a las amenazas. Estos agentes deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.

En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la Información y las Comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad.

El fortalecimiento de la ciberseguridad requiere un conocimiento sistemático sobre el impacto de una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales, así como métricas del nivel de seguridad de estos sistemas que permitan la oportuna toma de decisiones según su grado de exposición.

Objetivo II

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

El ciberespacio juega un papel cada vez más importante tanto en la comisión de hechos ilícitos o maliciosos como en su investigación para promover la confianza de los ciudadanos. Es necesario garantizar una adecuada persecución de los fenómenos criminales que en él se desarrollen.

Son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito.

CVE: BOD-2019-086-11358
Verificable en https://sede.defensa.gob.es/acceda/bod

Sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, así como la asignación de recursos suficientes a los órganos competentes en la materia y la capacitación de los profesionales que trabajan en este ámbito.

Del mismo modo, es fundamental fomentar la colaboración y participación ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés judicial y policial e identificando aspectos que requieran de una mejora en las capacidades de las instituciones policiales y de los organismos judiciales competentes.

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos

Todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Es por ello responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ciberseguridad es una responsabilidad compartida con los actores privados que, por acción u omisión, puedan afectarla; y no es posible conseguirla sin su participación. Por tanto, entre las medidas a impulsar deben estar aquellas que conduzcan a la necesaria cooperación para la seguridad común.

La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa. A la vez todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance.

La acelerada adopción por la sociedad de tecnologías emergentes provoca que los riesgos evolucionen. Por ello, el intercambio permanente de conocimiento con los diferentes actores y el establecimiento de mecanismos de monitorización para la protección del ecosistema empresarial y social serán instrumentos que permitirán al Gobierno estar informado y tomar las decisiones oportunas para actualizar y adecuar las acciones resultado de la presente estrategia.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con recursos técnicos y humanos que le proporcionen la autonomía tecnológica necesaria y la capacitación adecuada para el uso seguro del ciberespacio, situando a la ciberseguridad como habilitador clave para una nación emprendedora.

Para ello, debe mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas.

Se debe también contribuir al uso seguro y responsable de las Tecnologías de la Información y de las Comunicaciones promoviendo la capacitación en ciberseguridad de los profesionales adecuada a la demanda del mercado laboral, estimulando el desarrollo de los profesionales con habilidades propias, impulsando la formación y cualificación especializada, así como las capacidades de generación de conocimiento, el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados.

Asimismo, merece especial atención la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para promover la soberanía tecnológica y aprovechar

CVE: BOD-2019-086-11359
Verificable en https://sede.defensa.gob.es/acceda/bod

las oportunidades que ofrece la transformación digital, se fomentará e impulsará la industria española de ciberseguridad y las mejores prácticas en el desarrollo e implantación de sistemas de información y comunicaciones.

Objetivo V

Seguridad del ciberespacio en el ámbito internacional

España promoverá un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado.

Abogará por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

En línea con nuestros socios europeos, reforzará la confianza en Internet, en la transformación digital y en el desarrollo de las nuevas tecnologías, contribuyendo a consolidar un ecosistema cibernético europeo seguro que permita avances hacia el mercado único digital. Para ello defenderá un internet interoperativo, neutral, abierto y diverso, reflejo de la pluralidad cultural y lingüística internacional, basado en un sistema de gobernanza democrático, representativo e inclusivo, resultado de la concertación y el consenso. Además, un acceso a internet global y generalizado, contribuyendo con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

Del mismo modo, nuestra pertenencia a la Unión Europea (UE), nos obliga a fortalecer la seguridad y la autonomía estratégica europea mediante la búsqueda de sinergias, la cooperación técnica, operativa, estratégica y política; a reforzar nuestra resiliencia, nuestra capacidad de respuesta ante las crisis y las complementariedades entre los ámbitos civiles y militares como socios de la UE y aliados de la Organización del Tratado del Atlántico Norte (OTAN).

Sobre la base de lo anterior, España continuará participando activamente en la UE y la OTAN; en Naciones Unidas, y en sus foros derivados como el Foro de Gobernanza de Internet (IGF); en la Organización para la Seguridad y la Cooperación en Europa (OSCE), en el desarrollo e implementación de las Medidas de Fomento de la Confianza; en la Organización de Estados Americanos (OEA). Así como con el Foro Global del Expertos en Ciberseguridad (GFCE) y la Coalición por la Libertad en Internet (Freedom Online Coalition. FOC), sin olvidar nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE), así como en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

Además, reforzará la cooperación internacional bilateral en materia de ciberseguridad, promoverá relaciones fluidas y de confianza en este ámbito, colaborará en la construcción de capacidades en terceros Estados, prestando especial atención a las mujeres y los jóvenes y fomentará la creación de canales de información e intercambio de experiencias, impulsando, para todo ello, la adopción de acuerdos bilaterales y multilaterales en este ámbito.

CVE: BOD-2019-086-11360
Verificable en https://sede.defensa.gob.es/acceda/bod

CAPÍTULO 4

Líneas de acción y medidas

En este capítulo se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio:

Esta línea de acción responde al Objetivo I de la Estrategia.
Medidas:

1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.
2. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.
3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.
4. Asegurar la coordinación técnica y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.
5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.
6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.
8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.
9. Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.
10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.
11. Garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.
12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España:

Esta línea de acción responde al Objetivo I de la Estrategia.
Medidas:

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
3. Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la

CVE: BOD-2019-086-11361
Verificable en https://sede.defensa.gob.es/acceda/bod

normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo.

4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.

5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.

6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.

7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permita a las autoridades competentes determinar el nivel de seguridad y su evolución.

8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.

9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.

10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.

11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad, especialmente en áreas que puedan afectar a la Seguridad Nacional, la Administración pública, los servicios esenciales y las empresas cotizadas.

12. Asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i.

Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio:

Esta línea de acción responde al Objetivo II de la Estrategia.

Medidas:

1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.

2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.

3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.

4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.

5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha

CVE: BOD-2019-086-11362
Verificable en https://sede.defensa.gob.es/acceda/bod

contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.

6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.

7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

8. Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.

9. Fortalecer la cooperación judicial y policial internacional.

Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas:

Esta línea de acción responde al Objetivo III de la Estrategia.
Medidas:

1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.

3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la «identidad digital».

4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.

5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implantarán medidas de ciberdefensa activa de ciudadanos y pymes.

6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.

7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.

8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.

9. Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

Línea de Acción 5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital:

Esta línea de acción responde al Objetivo IV de la Estrategia.
Medidas:

1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a

CVE: BOD-2019-086-11363
Verificable en https://sede.defensa.gob.es/acceda/bod

programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.

2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.

3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.

4. Promover las actividades de normalización y la exigencia de requisitos ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.

5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.

8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.

9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales:

Esta línea de acción responde al Objetivo V de la Estrategia.

Medidas:

1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales y a los que pertenece y en los que la ciberseguridad forma parte sustancial de sus agendas, y apoyar y participar de manera activa en las diferentes iniciativas, coordinando la posición de los diferentes agentes nacionales implicados.

2. Promover en el ámbito de Naciones Unidas la búsqueda de consensos para el pleno respeto a la Carta de Naciones Unidas y la aplicación y puesta en práctica del Derecho Internacional y las normas para el comportamiento responsable de los Estados. Y del mismo modo avanzar en la adopción e implementación de Medidas para el Fomento de la Confianza en el ciberespacio.

3. Participar activamente en la Unión Europea en el desarrollo de un ecosistema europeo seguro que favorezca el avance y la consolidación del mercado único, y la seguridad y autonomía estratégica de Europa, buscando las complementariedades y la cooperación entre la Unión Europea y la OTAN.

4. Fomentar el diálogo bilateral, la cooperación y los sistemas de intercambio de información, alerta temprana y de experiencias para desarrollar un enfoque coordinado en la lucha contra las ciberamenazas con otros países, promoviendo la negociación y firma de acuerdos internacionales.

5. Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

CVE: BOD-2019-086-11364
Verificable en https://sede.defensa.gob.es/acceda/bod

6. Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países.

Línea de Acción 7. Desarrollar una cultura de ciberseguridad:

Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al objetivo IV de la Estrategia.

Medidas:

1. Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.
2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.
3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.
4. Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.
5. Promover un espíritu crítico en favor de una información veraz y de calidad y que contribuya a la identificación de las noticias falsas y la desinformación.
6. Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.
7. Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
8. Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

CAPÍTULO 5

La ciberseguridad en el Sistema de Seguridad Nacional

En este capítulo se contempla la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015 establecen una estructura orgánica específica para la ciberseguridad. En la presente Estrategia de 2019 se impulsan iniciativas que complementan los nuevos avances en el modelo de gobernanza nacional con las políticas europeas.

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

El Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

CVE: BOD-2019-086-11365
Verificable en https://sede.defensa.gob.es/acceda/bod

El Consejo de Seguridad Nacional actúa, a través del Departamento de Seguridad Nacional como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

El Comité de Situación:

El Comité de Situación tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.

El Consejo Nacional de Ciberseguridad:

El Consejo Nacional de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Entre sus funciones se encuentran reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilitar la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional, así como realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

La Comisión Permanente de Ciberseguridad:

La Comisión Permanente de Ciberseguridad se establece con objeto de facilitar la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.

El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis en el ámbito de la ciberseguridad. Dicho procedimiento establece sus funciones dirigidas a detectar y valorar los riesgos y amenazas; facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, e instrucciones para la gestión de la comunicación pública.

A fin de responder de manera oportuna y proporcionada a situaciones de especial relevancia en el desarrollo de sus funciones, se progresará en la definición de sus capacidades y responsabilidades.

Foro Nacional de Ciberseguridad:

Actuará en la potenciación y creación de sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas a la seguridad en el ciberespacio.

La puesta en marcha del foro Nacional de Ciberseguridad, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

CVE: BOD-2019-086-11366
Verificable en https://sede.defensa.gob.es/acceda/bod

Autoridades públicas competentes y los CSIRT de referencia nacionales:

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacional que se recogen en el marco jurídico nacional.

Asimismo, los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y sus organismos vinculados o dependientes, los de las entidades privadas, la red de CSIRT.es y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos. De igual modo, desde los CSIRT nacionales, en colaboración con los CSIRT autonómicos y privados, se fomentará la puesta en marcha de iniciativas que contribuyan a la consecución de los objetivos de la estrategia nacional.

Consideraciones finales y evaluación:

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en el presente documento una actualización de las amenazas y los desafíos a las que nos enfrentamos, siempre en continua evolución. Para adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Se elaborará un informe anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

(B. 86-1)

(Del *BOE* número 103, de 30-4-2019.)

CVE: BOD-2019-086-11367
Verificable en https://sede.defensa.gob.es/acceda/bod

I. — DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

PROTECCIÓN CIVIL

Orden PCI/488/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Protección Civil, aprobada por el Consejo de Seguridad Nacional.

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia Nacional de Protección Civil.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

Madrid, 26 de abril de 2019.–La Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, Carmen Calvo Poyato.

ANEXO

Estrategia Nacional de Protección Civil

Índice

CVE: BOD-2019-086-11368
Verificable en https://sede.defensa.gob.es/acceda/bod

CAPÍTULO 1

Una visión integral de la protección civil

1. *Introducción*

En un mundo global, cambiante e interdependiente, las causas y consecuencias de los distintos tipos de amenazas naturales o tecnológicas con efecto directo para las personas y sus bienes, traspasan fronteras. Esta realidad representa un desafío al que las estrategias y políticas públicas de protección civil no pueden resultar ajenas.

La evidencia científica indica que en el proceso histórico de evolución de la tierra se han producido alteraciones climáticas de diferente origen y naturaleza, que han transformado los mares en desiertos o que han provocado alteraciones en los ecosistemas

CVE: BOD-2019-086-11369
Verificable en https://sede.defensa.gob.es/acceda/bod

incidiendo en la extinción de algunas especies de animales y plantas, entre otros efectos. Sin embargo, en esta nueva era de desarrollo industrial el cambio climático viene marcado por el impacto directo de la actividad del hombre, lo que está provocando una alteración en el referido proceso.

Por otra parte, estamos ante un nuevo tiempo en el que los avances tecnológicos del último siglo han facilitado la comunicación global entre sociedades diversas y diferentes, en un mundo cada vez más conectado e interdependiente. En este contexto, la gestión integral de las emergencias supone un reto global que concierne a la comunidad internacional en su conjunto. La Estrategia Internacional para la Reducción de Desastres de las Naciones Unidas representa una herramienta de encuentro y consenso, para hacer frente a una situación que, a todos, en mayor o menor grado, concierne.

Pese al carácter global del desafío, la actividad principal dirigida a la reducción del riesgo de desastres tiene como primeros y principales responsables a los Estados y es precisamente en el ámbito nacional, de acuerdo con el marco de la citada Estrategia Internacional redefinida en Sendai en 2015 (Marco de Sendai), dónde se han de establecer y poner en práctica las políticas necesarias para hacer frente a las amenazas que nos afectan.

Esa responsabilidad de los Estados respecto de la seguridad de sus ciudadanos, aparece a su vez acompañada de la necesidad de transitar hacia una concepción que vaya más allá de la seguridad entendida en términos tradicionales. Un enfoque vinculado a la denominada «seguridad humana», que considere a los individuos como referentes centrales de su acción y que suponga también una ampliación respecto a las amenazas o riesgos que le afectan.

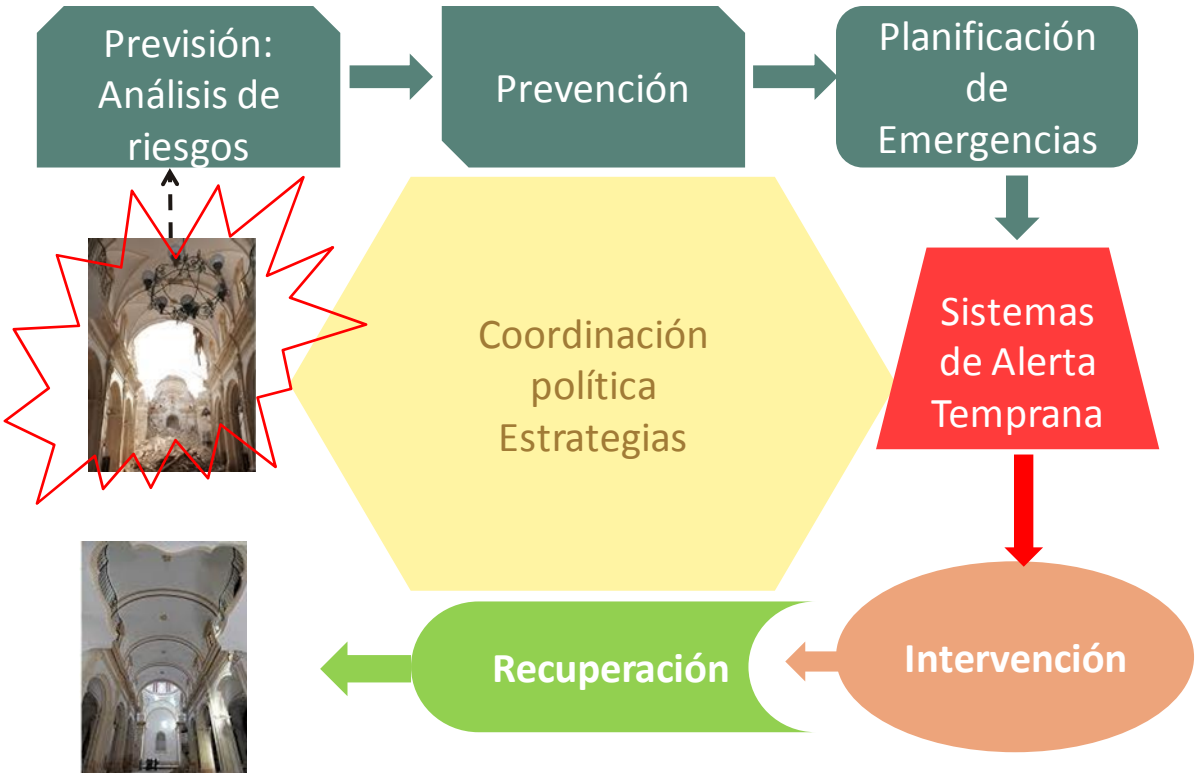
Para avanzar hacia una acción pública basada en esa seguridad humana, es preciso poner el foco en las políticas y servicios de protección civil, y en la importancia de considerar la diversidad de la sociedad sobre la que proyecta su actuación. Por este motivo, afrontar los nuevos escenarios y profundizar en la generación de una verdadera resiliencia social, exige de un enfoque estratégico que incorpore entre los factores potenciadores del riesgo aquellos condicionantes sociales, económicos o personales que pueden situar a las personas en una situación de especial vulnerabilidad ante las catástrofes y emergencias.

España es un país con un nivel global de riesgo moderado en su conjunto. Los incendios forestales, las inundaciones y aquellos derivados de la ocurrencia de fenómenos meteorológicos adversos, ocasionan periódicamente daños importantes que pueden llegar a afectar a la seguridad de las personas y sus bienes, contribuyendo, además, al deterioro del medio ambiente. En menor medida, están presentes, entre otros, los riesgos sísmicos, volcánicos y de origen tecnológico, si bien sus efectos pueden ser muy importantes en caso de producirse, por tratarse de eventos de baja probabilidad de ocurrencia, pero de alto impacto en sus consecuencias.

España cuenta con un sistema de protección civil adecuado para dar una respuesta eficaz y coordinada a las emergencias originadas por estos riesgos, que ha ido evolucionando hasta cristalizar, con la entrada en vigor de la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, en un sistema que ordena las acciones y políticas públicas en torno a los diferentes procesos del ciclo de las emergencias: anticipación, prevención, planificación, respuesta inmediata y recuperación. A este ciclo se incorpora el proceso de coordinación general de la acción política, tal y como se ilustra en la figura 1, siguiente.

CVE: BOD-2019-086-11370
Verificable en https://sede.defensa.gob.es/acceda/bod

Figura 1. El ciclo de gestión de las emergencias



La gestión de riesgos implica un conjunto de acciones de naturaleza compleja, que precisa de la coordinación del conjunto de las Administraciones públicas. En España, las competencias en este ámbito están distribuidas en tres niveles: Administración General del Estado, Comunidades Autónomas y Administración local, que actúan bajo los principios de solidaridad, complementariedad y subsidiariedad.

La compleja organización del Sistema Nacional de Protección Civil en el ámbito de la gestión de riesgos requiere una estrategia nacional concertada, como las que ya existen en otros campos de la actividad pública. Por ello, la referida Ley 17/2015, prevé, en su artículo 4 la elaboración de dos estrategias diferentes:

– Una Estrategia Nacional de Protección Civil que integrará y alineará todas las actuaciones de la Administración General del Estado en el ámbito de la protección civil, que debe ser aprobada por el Consejo de Seguridad Nacional a propuesta del Ministro del Interior.

– Una Estrategia del Sistema Nacional de Protección Civil que debe servir de base a las actuaciones de las distintas administraciones territoriales en el ámbito de sus respectivas competencias. Las líneas básicas de esta Estrategia del Sistema, las aprobará el Consejo Nacional de Protección Civil, máximo órgano de coordinación interadministrativa en este ámbito.

El presente documento, como Estrategia Nacional de Protección Civil, desarrolla un análisis de las principales amenazas y riesgos de origen natural, humano y tecnológico que pueden dar lugar a emergencias y/o catástrofes en nuestro país, así como las líneas de acción estratégicas para integrar, priorizar y coordinar todos los esfuerzos que permitan optimizar los recursos disponibles para su gestión.

CVE: BOD-2019-086-11371
Verificable en https://sede.defensa.gob.es/acceda/bod

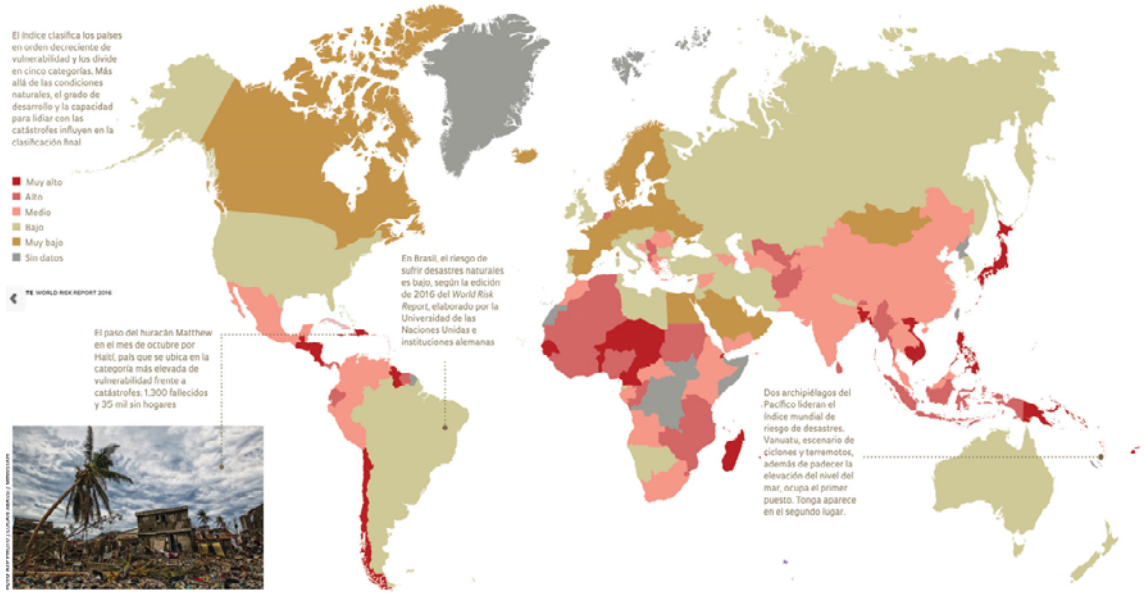
2. *Visión integral de la protección civil*

La presente Estrategia Nacional de Protección Civil parte de una visión integral de la protección civil, entendida esta como servicio público que protege a las personas y bienes garantizando una respuesta adecuada ante los distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana, sea esta accidental o intencionada.

La protección civil, como instrumento de la seguridad pública, ha tenido un eficaz desarrollo en los últimos años y se ha configurado como uno de los espacios públicos genuinos y legitimadores de la acción del Estado. Esto ha propiciado, sin duda, una paulatina reducción de la vulnerabilidad de la sociedad española ante las emergencias y catástrofes de origen natural y tecnológico.

Ahora bien, la constatación del aumento significativo, a nivel mundial, del número y gravedad de las emergencias y catástrofes en las últimas décadas (existiendo zonas geográficas de especial vulnerabilidad identificadas, tal y como se ilustra en la figura 2, siguiente) y la previsión de que estas ocasionen en el futuro efectos de mayor duración y alcance global como consecuencia del cambio climático, obliga a estar preparados para hacerles frente y adoptar un enfoque cada vez más integrado de su gestión.

Figura 2. Distribución geográfica de la vulnerabilidad frente a las emergencias (World Risk Report, 2017 UNU)



La protección civil en España, ha tenido en las últimas décadas un desarrollo importante y constante, no exento de dificultades de coordinación en un sistema con múltiples actores, abierto y flexible que le dota de una reconocida complejidad.

A lo largo de este periodo se han creado nuevos medios y recursos estatales, entre los que destaca la Unidad Militar de Emergencias (UME). Asimismo, las Fuerzas y Cuerpos de Seguridad del Estado han incrementado y potenciado sus capacidades y recursos en este ámbito, al objeto de poder dar una mejor respuesta desde el Estado a este tipo de situaciones. De igual manera, las Comunidades Autónomas y Entidades locales se han ido dotando de más y mejores recursos en el ámbito de sus competencias, sumando por tanto una mayor capacidad de respuesta ante las emergencias.

Este enfoque holístico de la protección civil a escala nacional, implica la necesidad de fortalecer permanentemente un Sistema Nacional de Protección Civil que integre la contribución de todas las administraciones, entidades privadas y ciudadanos. Igualmente, es necesario contemplar una dimensión internacional que refleje la demostrada vocación solidaria de la sociedad española.

CVE: BOD-2019-086-11372
Verificable en https://sede.defensa.gob.es/acceda/bod

3. *La protección civil como elemento esencial del Sistema de Seguridad Nacional*

La dimensión nacional de la protección civil se contempla en el marco de la Estrategia de Seguridad Nacional aprobada por el Consejo de Seguridad Nacional en 2017.

Tal y como ilustra la figura 3, siguiente, esta incluye a las emergencias y catástrofes como uno de los principales desafíos del mundo moderno, pues su impacto no solo afecta a la vida y salud de las personas sino, también a los bienes patrimoniales, al medioambiente y al desarrollo económico.

Figura 3. Amenazas y desafíos para la seguridad nacional
(Estrategia de Seguridad Nacional 2017)

Consecuentemente, la Estrategia de Seguridad Nacional incluye como objetivo la consolidación del Sistema Nacional de Protección Civil en cuanto instrumento integrador de todas las capacidades nacionales en la gestión de las emergencias y catástrofes (cuyos principales elementos y estructuración se recogen en la figura 4, siguiente), así como asegurar su integración en el Sistema de Seguridad Nacional configurado por la Ley 36/2015, de 28 de septiembre.

CVE: BOD-2019-086-11373
Verificable en https://sede.defensa.gob.es/acceda/bod

Figura 4. Estructuración de las capacidades del Sistema Nacional de Protección Civil

En este contexto integrador, España debe fomentar, dentro de la cultura de Seguridad Nacional, la concienciación ciudadana sobre las principales amenazas y riesgos que pueden provocar situaciones de índole catastrófica. Para ello, resulta esencial potenciar las conductas de autoprotección y resiliencia de la sociedad española. En definitiva, una protección civil eficaz requiere de la sensibilización social de los ciudadanos, como destinatarios de la acción pública dirigida a afrontar tales situaciones.

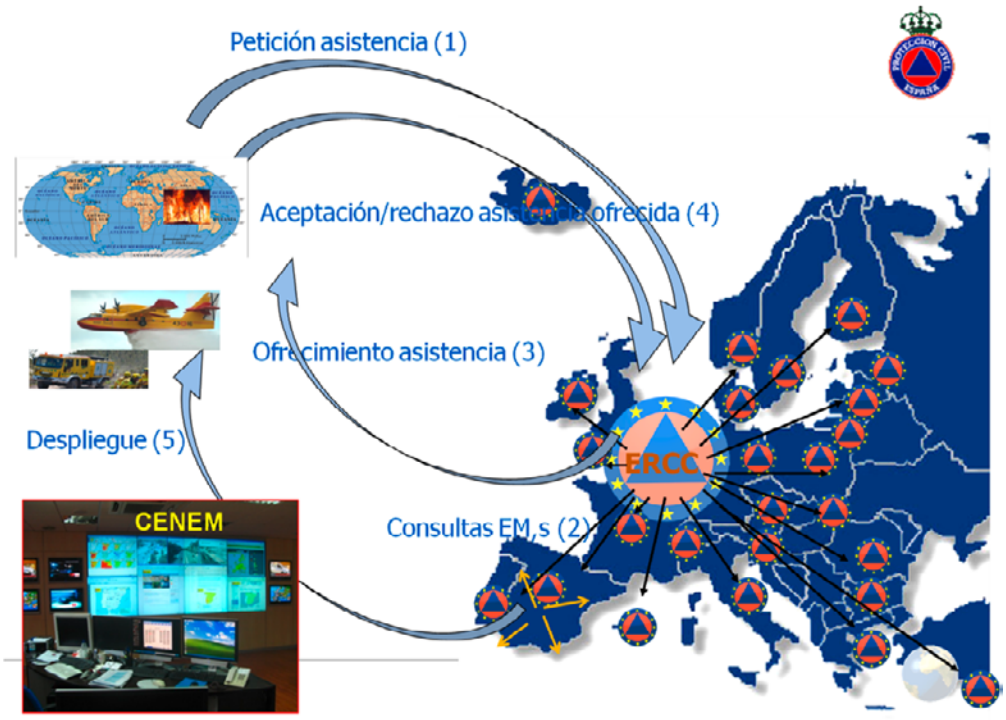
4. *La protección civil en la agenda internacional*

España tiene una clara identidad europea, mediterránea y atlántica que confiere una dimensión internacional a su protección civil y que proyecta hacia el exterior la solidaridad del conjunto de la sociedad española a la hora de cooperar para prevenir, aliviar y paliar los efectos de los desastres que afecten a otros países.

Como muestra de esta vocación internacional, España es miembro relevante del Mecanismo de Protección Civil de la Unión Europea, regulado por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo (cuyas líneas generales de actuación se ilustran en la figura 5, siguiente), que es el instrumento que fomenta la solidaridad apoyando, complementando y facilitando la coordinación entre los Estados miembro, con la finalidad de mejorar la eficacia de los sistemas de prevención, preparación y respuesta ante catástrofes naturales o de origen humano.

CVE: BOD-2019-086-11374
Verificable en https://sede.defensa.gob.es/acceda/bod

Figura 5. Secuencia activación del Mecanismo Europeo de Protección Civil



El Mecanismo se encuentra actualmente en proceso de revisión, para mejorar su eficacia en la prevención y respuesta ante emergencias. Como líneas más relevantes de la nueva estructura cabe mencionar la dotación de una nueva reserva de capacidades gestionadas directamente por la Unión Europea (rescUE), así como la racionalización y simplificación de los procedimientos administrativos al objeto de reducir el tiempo necesario para la movilización de los recursos de la capacidad europea de respuesta en emergencias. A esta capacidad España contribuye significativamente con módulos y equipos del Sistema Nacional de Protección Civil.

Además, España mantiene un ámbito de colaboración mediante convenios bilaterales con los países europeos de nuestro entorno (Francia y Portugal) y con los del sur del Mediterráneo (Argelia, Túnez y Marruecos) que refuerzan la cooperación y ayuda mutua para hacer frente a las amenazas y riesgos que compartimos.

En el ámbito de Naciones Unidas, España ha adoptado el ya citado Marco de Sendai para la Reducción del Riesgo de Desastres 2015-2030 como principal compromiso internacional, que persigue la reducción sustancial del riesgo de desastres y de las pérdidas ocasionadas por los mismos.

CVE: BOD-2019-086-11375
Verificable en https://sede.defensa.gob.es/acceda/bod

Finalmente, y en línea con las estrechas relaciones con los países iberoamericanos, España ostenta la Secretaría permanente de la Asociación Iberoamericana de Organismos Gubernamentales de Defensa y Protección Civil, creada en Santiago de Chile en julio de 1996, que persigue como objetivo el fomento de la cooperación científica y técnica en materia de gestión de desastres y el incremento y mejora del intercambio de información y experiencias.

En resumen, la complejidad y transversalidad en la gestión de las emergencias y catástrofes que ocurren con frecuencia creciente, no solo ha motivado la adopción de un enfoque basado en la cooperación entre los actores competentes de ámbito nacional sino también internacional, lo cual ha tenido un importante impacto en el desarrollo de las diferentes políticas públicas en materia de protección civil. La experiencia acumulada por nuestro país a este respecto en las últimas décadas permite hablar de una situación de reconocimiento y peso específico de la protección civil española en la escena internacional.

CAPÍTULO 2

El Sistema Nacional de Protección Civil, parte esencial del Sistema de Seguridad Nacional

1. *El Sistema de Seguridad Nacional*

El Sistema de Seguridad Nacional, tal y como ilustra la figura 6, siguiente, ha sido configurado por la Ley 36/2015, de 28 de septiembre, como un conjunto de órganos, organismos, recursos y procedimientos que, dirigidos por el Presidente del Gobierno, permiten orientar la acción del Estado para asegurar la protección de la libertad, los derechos y el bienestar de los ciudadanos, la garantía de la defensa de España y de sus principios y valores constitucionales, y la contribución con nuestros aliados al fortalecimiento de la seguridad internacional, frente a las transversales y complejas amenazas que las sociedades actuales se ven obligadas a afrontar.

CVE: BOD-2019-086-11376
Verificable en https://sede.defensa.gob.es/acceda/bod

Figura 6. El Sistema de Seguridad Nacional

El Sistema se organiza en torno a un órgano principal y un órgano de apoyo de trabajo permanente. El primero de ellos es el Consejo de Seguridad Nacional, Comisión Delegada del Gobierno para la Seguridad Nacional que asiste al Presidente del Gobierno en la dirección de esta política estatal. El segundo es el Departamento de Seguridad Nacional, que asesora al Presidente del Gobierno en materia de Seguridad Nacional.

Como refleja la figura 7, siguiente, el Presidente del Gobierno preside este Consejo en el que se integran, además de los representantes de las carteras ministeriales relacionadas con la gestión de crisis, otras autoridades estatales, como por ejemplo la Secretaría de Estado de Comunicación, autonómicas, o incluso personas físicas o jurídicas, cuando fuere precisa su asistencia por la naturaleza de los temas a tratar.

Figura 7. Composición y estructura del Consejo de Seguridad Nacional

CVE: BOD-2019-086-11377
Verificable en https://sede.defensa.gob.es/acceda/bod

El Consejo de Seguridad Nacional puede crear órganos que le apoyen en el desempeño de sus funciones en ámbitos determinados de la Seguridad Nacional, que reciben la denominación de Comités Especializados u otros que así se determinen. Además, el Departamento de Seguridad Nacional (DSN), ejerce las funciones de secretaría técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo.

La gestión de las situaciones de crisis es el conjunto ordinario de actuaciones dirigidas a detectar y valorar las amenazas y riesgos concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada del Estado.

Para garantizar una eficaz respuesta, el Consejo de Seguridad Nacional cuenta con el apoyo del Comité de Situación, presidido por la Vicepresidenta del Gobierno o excepcionalmente, a decisión del Presidente del Gobierno, por la autoridad funcional que el mismo designe. Especial atención requieren aquellas que pudieran derivar en una declaración de Situación de Interés para la Seguridad Nacional, por parte del Presidente del Gobierno.

2. *Relación entre el Sistema Nacional de Protección Civil y el Sistema de Seguridad Nacional*

La actual Estrategia de Seguridad Nacional 2017, marco político-estratégico de referencia de la Política de Seguridad Nacional que describe las principales amenazas y riesgos para la Seguridad Nacional, considera como uno de los ámbitos principales la protección ante emergencias y catástrofes.

Además, como se ilustra en la figura 8, siguiente, contempla una serie de factores que potencian el impacto de las emergencias y catástrofes en la Seguridad Nacional, como son el demográfico, motivado por el incremento de población urbana en zonas de peligro ambiental; la vulnerabilidad de la infraestructura económica y tecnológica, que acentúa la rapidez y propagación de los riesgos y genera efectos en cascada; la degradación de los ecosistemas, que reduce las defensas naturales; y el incremento de la magnitud y frecuencia de algunos fenómenos adversos como consecuencia del cambio climático.

Figura 8. Potenciadores del impacto de emergencias y catástrofes.

Por otra parte, en la Estrategia de Seguridad Nacional 2017, se incluyen como líneas de acción de la Seguridad Nacional en el ámbito de las emergencias y catástrofes, entre otras, la elaboración de una Estrategia Nacional de Protección Civil, el desarrollo reglamentario de la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, el fortalecimiento de la integración de capacidades del Sistema Nacional de Protección Civil mediante la cooperación y coordinación entre todas las Administraciones Públicas competentes, así como la coordinación y cooperación internacional en la materia.

El Sistema Nacional de Protección Civil está, por tanto, plenamente integrado en el Sistema de Seguridad Nacional, como se refleja en la figura 9, siguiente. De esta manera,

CVE: BOD-2019-086-11378
Verificable en https://sede.defensa.gob.es/acceda/bod

la regulación establecida en la referida Ley se aplica sin perjuicio de lo dispuesto por la normativa vigente para el Sistema de Seguridad Nacional. Además, el Consejo de Seguridad Nacional ostenta la competencia para la aprobación, a propuesta del Ministro del Interior, de la Estrategia Nacional de Protección Civil.

Figura 9. Integración del Sistema Nacional de Protección Civil en el Sistema de Seguridad Nacional

Asimismo, la Ley 17/2015 establece que la dirección de las emergencias de interés nacional, que exige la ordenación y coordinación de las actuaciones y la gestión de todos los recursos nacionales e internacionales, es competencia del Ministro del Interior.

El Departamento de Seguridad Nacional realizará el seguimiento intensivo de dicha situación. Además, en función de su evolución y gravedad, el Consejo de Seguridad Nacional podrá proponer al Presidente del Gobierno la activación plena del Sistema de Seguridad Nacional, así como la posible declaración de una Situación de Interés para la Seguridad Nacional, sin perjuicio de las actuaciones propias del Sistema Nacional de Protección Civil.

Como conclusión, debe señalarse que la integración del Sistema Nacional de Protección Civil en el Sistema de Seguridad Nacional permite al Gobierno de la Nación afrontar la gestión de las amenazas y los riesgos con un enfoque integral.

CAPÍTULO 3

Amenazas y riesgos en el ámbito de la protección civil

1. *Introducción*

En un mundo global como el actual, coexisten las amenazas y riesgos tradicionales cuyas consecuencias son conocidas en función de la experiencia adquirida, con los llamados riesgos emergentes, ante los que nos encontramos con una mayor incertidumbre para la valoración de su gravedad y alcance potencial.

Tres rasgos fundamentales caracterizan hoy a la denominada sociedad del riesgo. El primero es su carácter transnacional, debido fundamentalmente al efecto de la globalización, que hace que sus consecuencias no se limiten a un lugar o espacio geográfico definido.

CVE: BOD-2019-086-11379
Verificable en https://sede.defensa.gob.es/acceda/bod

El segundo es la forma creciente e interdependiente en la que determinadas tendencias y factores, tales como la demografía, los condicionantes socioeconómicos y personales, el cambio climático y las nuevas orientaciones en los desarrollos industriales, inciden sobre las consecuencias de las emergencias y catástrofes para la población afectada.

El tercer rasgo observado es el carácter asimétrico de las nuevas amenazas y de sus agentes, que han ido surgiendo en paralelo al desarrollo de la sociedad moderna.

Las amenazas y riesgos no solo se ven afectados por condicionantes de carácter global, sino que las circunstancias o características específicas locales, relativas a cuestiones geográficas, históricas, políticas, económicas y sociales, determinan la manera en que esos condicionantes actúan como factores potenciadores.

El deterioro del medio ambiente y el cambio climático son quizás los desafíos más importantes del siglo XXI, que únicamente a partir de la década de los años setenta comenzaron a tratarse desde un enfoque internacional. Las soluciones a estos problemas no son fáciles, porque el deterioro del medio ambiente está, en buena medida, asociado a un modo de vida basado en el consumo y el crecimiento. Por su parte, el cambio climático provocado por la quema de combustibles fósiles y la deforestación, conllevará en España un aumento de la desertificación, una reducción de los recursos hídricos y la pérdida de biodiversidad, entre otros efectos.

De la experiencia adquirida en la prevención, gestión, recuperación y seguimiento de los diferentes episodios de emergencia, se desprenden las principales tendencias de los últimos años. Un periodo que se ha caracterizado por una gran variabilidad meteorológica y crecientes desajustes estacionales, que dificultan los procesos de predicción y se traducen en episodios atemporales de fuertes contrastes. Por un lado, se han producido etapas de fuerte sequía meteorológica e hidrológica y temperaturas extremas en zonas poco habituales. Por otro, se han experimentado cuadros de lluvias torrenciales durante el verano y otoño, que han generado episodios de inundaciones, así como intensas nevadas. Este tipo de episodios constituyen el fenómeno natural que más daños materiales causa en España y en Europa.

Por otra parte, la importancia de los incendios forestales en nuestro país guarda relación con un clima eminentemente mediterráneo como España. El resultado de las políticas públicas en esta materia, unido a la generación paulatina de una mayor concienciación ciudadana que incluye el rechazo de la opinión pública a cierto tipo de prácticas de riesgo, permite mantener una tendencia decreciente en cuanto a número de incendios y superficie quemada, si bien sigue siendo un riesgo elevado en nuestro país, riesgo que tenderá a agravarse en el futuro como consecuencia del cambio climático.

En cuanto a los efectos de la actividad sísmica y volcánica, aunque España no es una zona especialmente expuesta a estos fenómenos, sí son frecuentes los movimientos sísmicos en determinadas zonas. Si bien su ocurrencia con consecuencias catastróficas es de baja probabilidad, en caso de producirse, genera un elevado impacto sobre la población afectada, sus bienes y las infraestructuras.

Finalmente, por lo que respecta a los sucesos relacionados con los riesgos tecnológicos, cabe destacar que en los últimos años se han mantenido en niveles moderados de ocurrencia.

Como conclusión se puede señalar que, la evolución de las amenazas globales, unida a la particular posición geográfica de España, hacen que las consecuencias de este tipo de fenómenos deban ser considerados, por sus posibles efectos en términos de Seguridad Nacional, tal y como se establece en el preámbulo de la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.

2. *Riesgos: Identificación y análisis*

Los riesgos más relevantes a efectos de la presente Estrategia Nacional de Protección Civil, de entre los citados en la Ley 17/2015, son los siguientes:

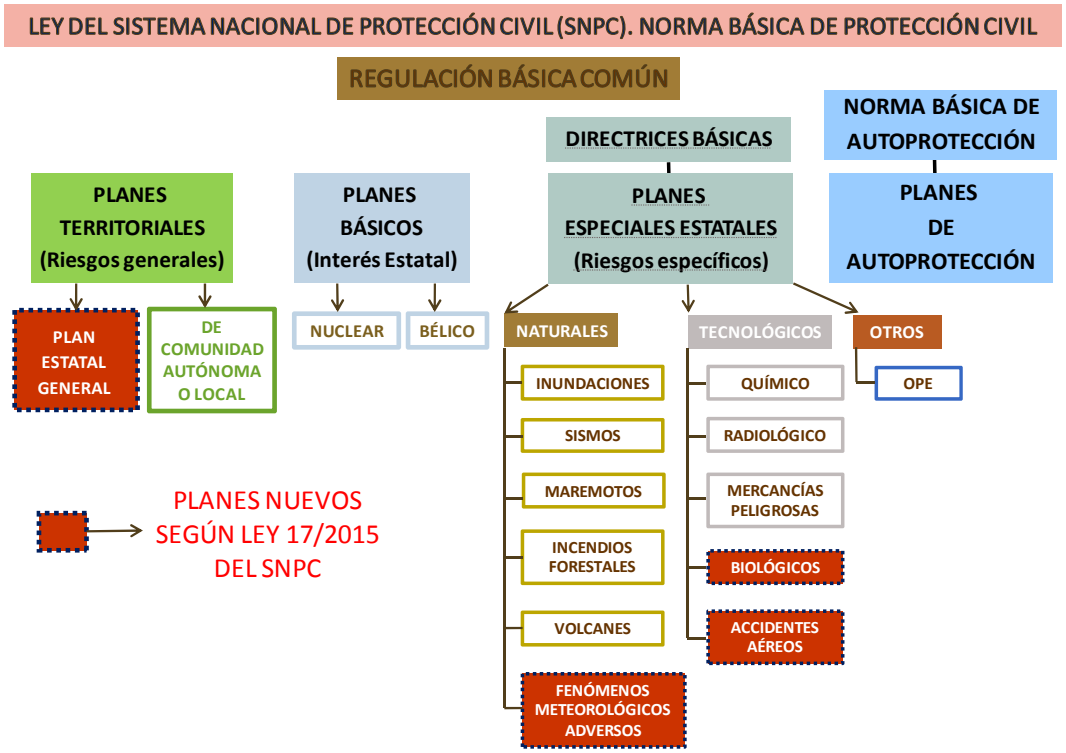
– Inundaciones.
– Incendios forestales.

CVE: BOD-2019-086-11380
Verificable en https://sede.defensa.gob.es/acceda/bod

– Terremotos y maremotos.
– Volcánicos.
– Fenómenos meteorológicos adversos.
– Accidentes en instalaciones o procesos en los que se utilicen o almacenen sustancias peligrosas.
– Transporte de mercancías peligrosas por carretera y ferrocarril.
– Nuclear y radiológico.

Para afrontar los mencionados riesgos, como recoge la figura 10, siguiente, se dispone de planes territoriales y especiales, de naturaleza estatal, autonómica y local, en función de su ámbito competencial y territorial. Dichos planes serán aprobados por la Administración competente en cada caso.

Figura 10. Tipos de planes en materia de Protección Civil



3. *Potenciadores del riesgo*

– El cambio climático: Según las conclusiones del último informe de evaluación del Grupo Intergubernamental de Expertos sobre el Cambio Climático (IPCC) de Naciones Unidas, el cambio climático provocará un aumento de la frecuencia o de la intensidad de eventos extremos vinculados al clima, como olas de calor y precipitaciones. En los países del área mediterránea se incrementará la frecuencia de las olas de calor y las sequías, así como las condiciones meteorológicas que propician los grandes incendios forestales.
– Deficiente ordenación territorial y asignación de usos del suelo: La escasa y tardía incorporación de los riesgos como condicionante restrictivo de la asignación de usos del suelo en los planes de ordenación territorial y urbana, ha incrementado la vulnerabilidad social y económica. Se han identificado situaciones problemáticas como la ocupación de cauces fluviales y de zonas de protección del dominio público hidráulico, la intensa presión antrópica sobre el litoral que concentra un gran porcentaje de la población española, la presencia de infraestructuras que obstaculizan los procesos naturales, o la impermeabilización de suelos por actuaciones urbanísticas intensivas, entre otras.

CVE: BOD-2019-086-11381
Verificable en https://sede.defensa.gob.es/acceda/bod

– Globalización: El aumento y la extensión de las comunicaciones, ha permitido un constante aumento del intercambio cultural, económico, social y político a nivel internacional, haciendo con ello un mundo más interconectado y dependiente. Algunas consecuencias de este fenómeno, como las que pudieran derivar del incremento del flujo en los transportes de mercancías y viajeros, entre otras, explican su consideración como factor potenciador de determinados riesgos y amenazas.

– Condicionantes socioeconómicos y demográficos: La construcción en ramblas o cauces secos, los problemas en la aplicación de normativa de construcción sismo-resistente, la acumulación de combustibles en los montes, la tendencia al crecimiento de usos recreativos en zonas peligrosas (montaña, barrancos, bosques, etc.), la deforestación, el abandono creciente del pastoreo en los bosques, los cultivos en suelos inadecuados, el aumento del interfaz urbano-forestal, la percepción del riesgo por parte de la población o la reducción y envejecimiento de la población rural, son algunos de los condicionantes socioeconómicos y demográficos que actúan como factores potenciadores del riesgo.

– Singularidades geográficas y climáticas: España se caracteriza por un relieve accidentado, diversidad de climas, presencia de cauces torrenciales, ocurrencia de fenómenos meteorológicos y climáticos extremos (gota fría, ciclo-génesis, olas de calor, etc.), intensos procesos de erosión y desertización, y la presencia de áreas de alta peligrosidad sísmica.

– Colectivos en situación de especial vulnerabilidad: La existencia de grupos de población en situación de especial vulnerabilidad (por sus características personales, sociales o económicas) requiere que dicha circunstancia sea tomada en consideración a la hora de valorar el riesgo y plantear la respuesta de los poderes públicos ante los mismos. El paulatino envejecimiento de la población española es otro elemento a considerar, por su posible impacto en la vulnerabilidad personal frente a algunos tipos de riesgos.

4. *Descripción de los riesgos*

4.1 Inundaciones.

4.1.1 Descripción: En España la pluviosidad media no es muy abundante, pero en ocasiones se producen precipitaciones que en muy pocas horas alcanzan valores muy extremos. Estas lluvias extraordinarias provocan caudales extremos, que al circular por el terreno pueden dar lugar a crecidas, avenidas o riadas, desbordando su cauce habitual, provocando la inundación de terrenos, y afectando a personas y bienes.

La gran variabilidad entre los caudales ordinarios y extraordinarios de algunos ríos, en ocasiones de forma súbita y la ocupación desordenada de los márgenes de los cauces, hace que el problema de las inundaciones revista en España una especial gravedad.

Las avenidas súbitas, provocadas por lluvias torrenciales, de corta duración, gran intensidad y muy localizadas, son un fenómeno bastante frecuente en España produciendo pérdida de vidas humanas, unas 300 en los últimos 30 años, y cuantiosos daños materiales que pueden estimarse en unos 500 millones de euros anuales.

Por otra parte, los temporales de varios días de duración que afectan a grandes cuencas producen otro tipo de inundación más lenta, que causan fundamentalmente daños económicos y, más infrecuentemente, personales.

Aunque las crecidas son, en su origen, un fenómeno natural eminentemente físico e hidrológico, en su desarrollo sobre zonas donde hay actividades humanas se convierte en un problema relacionado con la ordenación del territorio que presenta importantes repercusiones sociales y económicas.

4.1.2 Potenciadores: La ocupación intensiva del territorio da lugar a una alta exposición de las poblaciones. Si a ello se une el aumento de la frecuencia e intensidad de las precipitaciones extremas motivadas por el cambio climático, tendremos identificados los principales factores potenciadores del riesgo de inundaciones en España.

4.1.3 Instrumentos normativos y de gestión:

– En el marco europeo, el Parlamento aprobó la Directiva 2007/60/CE relativa a la evaluación y gestión de los riesgos de inundación. Esta Directiva tuvo su transposición en

CVE: BOD-2019-086-11382
Verificable en https://sede.defensa.gob.es/acceda/bod

el ordenamiento jurídico español a través del Real Decreto 903/2010, de 9 de julio, de evaluación y gestión de riesgos de inundación.

– La directriz básica de emergencias ante el riesgo de inundaciones (aprobada por Acuerdo de Consejo de Ministros de 9 de diciembre de 1994 y publicada en el BOE de 14 de febrero de 1995), establece el marco sobre el que se han desarrollado los planes especiales de protección civil de ámbito estatal y autonómico, donde se relaciona expresamente el nivel del riesgo de inundación del territorio con la planificación territorial y los usos del suelo.

– Plan Estatal de Inundaciones, aprobado por Acuerdo de Consejo de Ministros de 29 de julio de 2011.

4.1.4 Actuaciones prioritarias:

– Fortalecer la vinculación de la planificación de protección civil en los planes de ordenación del territorio, uso del suelo y desarrollo urbanístico.

– Promover el uso del Sistema Nacional de Cartografía de zonas inundables, identificando los elementos más vulnerables a efectos de protección civil en dichas áreas.

– Fortalecer los Sistemas de Aviso Hidrológico de los Organismos de Cuenca, desarrollando equipos y herramientas predictivas de fenómenos adversos, especialmente en aquellos casos susceptibles de causar inundaciones.

– Fomentar el desarrollo de nuevas herramientas predictivas de fenómenos meteorológicos extremos, especialmente en aquellos casos susceptibles de causar inundaciones.

4.2 Incendios forestales.

4.2.1 Descripción: Los incendios forestales se producen de forma periódica y recurrente todos los años en España. Su número, en términos absolutos, es muy elevado en comparación con los países de la UE, si bien se trata del segundo país europeo en extensión de la superficie forestal, y el cuarto en superficie ocupada por masas arboladas.

Al elevado número de incendios y extensión de la superficie forestal se suma el aumento de la intensidad con que estos se producen. Por término medio, un 34 % de la superficie quemada cada año, es consecuencia de unas pocas decenas de incendios, que presentan dimensiones superiores a las 500 has. Son los denominados grandes incendios.

Los incendios forestales, por tanto, constituyen un grave problema, tanto por los daños que ocasionan de modo inmediato en las personas y bienes, como por la grave repercusión que tiene la destrucción de extensas masas forestales sobre el medio ambiente.

Los incendios forestales son la causa más importante de degradación de los ecosistemas forestales, provocando elevados daños ecológicos y económicos e incluso pérdida de vidas humanas, por lo que requieren una atención preferente para gestionarlos de modo que se reduzca su ocurrencia, su incidencia y sus consecuencias.

El número de incendios que se inicia cada año y las superficies afectadas, continúan representando una amenaza recurrente para las personas, sus bienes y el medioambiente. Así mismo, el creciente grado de desarrollo urbano en los entornos forestales (interfaz urbano-forestal), hace que los incendios forestales ocurridos en estas zonas representen un riesgo especialmente grave debido a las peculiaridades y complejidad que entraña su extinción.

4.2.2 Potenciadores:

– El clima dominante en el área mediterránea con prolongadas sequías acompañadas de altas temperaturas estivales y, en ocasiones, de fuertes vientos, propicia unas condiciones meteorológicas favorables para que se produzcan incendios forestales.

– La Estadística General de Incendios Forestales, si bien muestra una tendencia global de descenso el número de incendios y superficies afectadas por los mismos, apunta a que el problema sigue siendo cíclico y recurrente y con una evolución futura que puede verse condicionada especialmente por el fenómeno del cambio climático; de hecho, el cambio climático está amplificando el impacto de eventos meteorológicos extremos en Europa, lo que conllevará por tanto escenarios que apuntan a un incremento en los índices

CVE: BOD-2019-086-11383
Verificable en https://sede.defensa.gob.es/acceda/bod

de riesgo y la intensidad de los incendios, incluso fuera de las épocas habituales, en especial en el sur de Europa.

– La ocurrencia de incendios forestales fuera de estación dificulta la planificación para la lucha y mantenimiento de servicios permanentes y especializados en la extinción de incendios.

– Otro potenciador lo constituyen los condicionantes socioeconómicos y demográficos, la pérdida de valor de los productos forestales, la despoblación de las áreas rurales y el aumento de la población urbana, que tiene como consecuencia el aumento de tierras agrícolas abandonadas –con el consiguiente aumento de masa forestal combustible–, todo lo cual representa un problema añadido para una gestión eficiente y sostenible del monte.

– Así mismo, el uso indiscriminado del fuego para el mantenimiento de pastos, la acción intencionada o interesada y el uso recreativo del monte por población eminentemente urbana, constituyen otro factor potenciador de este riesgo.

4.2.3 Instrumentos normativos y de gestión:

– La Ley 21/2015, de 20 de junio, por la que se modifica la Ley 43/2003, de 21 de noviembre, de Montes.

– Anualmente, el Gobierno aprueba el Plan de Actuaciones de Prevención y Lucha contra Incendios forestales, en el que se desarrollan medidas de entre varios ministerios con vocación unificadora integral y coordinadora de la política estatal en la materia.

– El Real decreto 893/2013, de 21 de noviembre, aprobó la directriz básica ante el riesgo de incendios forestales que fija los criterios y contenidos de la planificación de emergencias a nivel estatal y autonómico.

– El Plan Estatal de Protección Civil para Emergencias por Incendios Forestales, aprobado por Acuerdo de Consejo de Ministros 24 de octubre de 2014.

– Los planes especiales de protección civil de las Comunidades Autónomas para la respuesta a emergencias derivadas de este riesgo.

– El Comité de Lucha contra Incendios Forestales, Comité técnico de cooperación formado por representantes de todas las Administraciones competentes en materia de incendios forestales.

4.2.4 Actuaciones prioritarias:

– Identificar las capacidades mínimas de extinción del Sistema Nacional de Protección Civil, para su uso coordinado a nivel estatal e internacional.

– Reforzar la acción pública para garantizar el cumplimiento de la Ley, y en particular, la persecución y esclarecimiento del delito, fomentando la colaboración ciudadana.

– Promover la elaboración de los planes autoprotección de las instalaciones y actividades que tengan lugar en el terreno urbano-forestal.

– Fortalecer las capacidades operativas y de prevención en el ámbito local, ante los incendios de la interfaz urbano-forestal.

– Incentivar la formación en protocolos de actuación ante incendios de la población rural en territorios eminentemente forestales.

– Potenciar la formación de los intervinientes en incendios forestales.

4.3 Terremotos y maremotos.

4.3.1 Descripción: La península Ibérica se halla situada en el borde sudoeste de la placa Euroasiática en su colisión con la placa Africana. Nuestro país no presenta un área de grandes terremotos, aunque sí tiene una actividad sísmica relevante con sismos de magnitudes moderadas capaces de generar daños muy graves.

Se registran anualmente en la Península Ibérica unos 6.000 sismos, en la mayoría de los casos de baja magnitud, que se concentran al sur de la línea Cádiz-Alicante y en el área pirenaica, principalmente.

Mención especial merecen el terremoto de Lorca, ocurrido el 11 de mayo de 2011, que causó 9 víctimas mortales y 324 heridos, además de daños estructurales a más de un millar de edificios y al importante patrimonio cultural de la ciudad.

CVE: BOD-2019-086-11384
Verificable en https://sede.defensa.gob.es/acceda/bod

No existe actualmente ningún método capaz de predecir con precisión el tiempo, lugar y magnitud de un sismo, aunque si pueden delimitarse las zonas de mayor peligro basándose en los registros históricos y los condicionantes geológicos.

Es necesario, por ello, avanzar en la articulación de medidas preventivas como la adopción y el efectivo cumplimiento de normas de construcción sismo-resistente adaptadas a la geografía que el riesgo presente.

En este apartado es también preciso hacer referencia al riesgo de maremotos, muy poco probable en nuestro entorno, pero con un gran impacto potencial, tal como ocurriera en el conocido como terremoto de Lisboa de 1755, que produjo una gran ola que afectó a toda la costa atlántica española, especialmente a las provincias de Cádiz y Huelva, a la que se añadieron las consecuencias directas del terremoto. No puede tampoco descartarse la ocurrencia del mismo fenómeno, con menor intensidad, en la costa mediterránea e Islas Baleares, a causa de la sismicidad del norte de África, tal como ocurriera en el año 2003. (terremoto de Boumerdès, Argelia)

Finalmente, no es extraño que el fenómeno sísmico se presente en forma de un elevado número de terremotos de muy baja o baja intensidad, registrados en la misma zona geográfica durante un periodo continuado de tiempo, y que se prolongue durante semanas o meses. Aunque este fenómeno, denominado enjambre sísmico, no ha provocado daños personales ni materiales de consideración, si los terremotos son sentidos por la población producen una alarma social considerable por la incertidumbre de su evolución y sobre todo, cuando su origen se atribuye a causa de la actividad humana. La sismicidad ocurrida en la costa de Castellón en 2013, cuyo origen se atribuyó a la planta de almacenamiento de gas existente frente a sus costas, fue ejemplo de ello.

4.3.2 Potenciadores:

– Factores socioeconómicos que, en el pasado, llevaron al crecimiento desordenado del parque edificado, con una deficiente o inexistente normativa de construcción sismo-resistente, que hizo aumentar la exposición a este riesgo, en especial en las áreas más expuestas, que en muchos casos coinciden con zonas turísticas de alta ocupación.

– El desconocimiento o falta de estudios locales de la respuesta sísmica del suelo que permitan a la escala adecuada zonificar el territorio en aras de condicionar el planeamiento urbanístico y limitar los usos del suelo. A ello se añade la vulnerabilidad del parque inmobiliario rural.

– La concentración de población en áreas turísticas expuestas en determinadas épocas del año, que puede producir un desequilibrio entre los medios y recursos de respuesta y el tamaño de la población a atender.

– El alto periodo de retorno de los terremotos destructivos y/o maremotos, hace que la población tenga una percepción baja del riesgo, aumentando su vulnerabilidad.

4.3.3 Instrumentos normativos y de gestión:

– La directriz básica de protección civil ante el riesgo sísmico fue aprobada por Acuerdo del Consejo de Ministros del 7 de abril de 1995. En ella se consideran dos niveles de planificación: el estatal y el de Comunidad Autónoma, incluyendo en este último los Planes de Actuación que sean confeccionados por las entidades locales.

– La directriz básica de protección civil ante el riesgo de maremotos fue aprobada por Acuerdo del Consejo de Ministros del 20 de noviembre de 2015.

– El Plan Estatal ante el riesgo sísmico, aprobado por Acuerdo del Consejo de Ministros del 26 de marzo de 2010. En él se establece la organización y los procedimientos de actuación.

– Real Decreto 953/2018, de 27 de julio, recoge en su artículo 15, las funciones y competencias encomendadas a la Dirección General del Instituto Geográfico Nacional (IGN), y en particular en el apartado c) establece como competencia del IGN la planificación y gestión de sistemas de detección y comunicación a las instituciones de los movimientos sísmicos ocurridos en territorio nacional y sus posibles efectos sobre las costas.

CVE: BOD-2019-086-11385
Verificable en https://sede.defensa.gob.es/acceda/bod

– Los Planes Especiales ante el Riesgo Sísmico de las Comunidades Autónomas obligadas por la normativa a realizarlo (aquellas en las que son previsibles terremotos de intensidad igual o superior a VI).

– La norma sismo resistente para edificación, NCSE-02 fue publicada en el BOE de 11 de octubre de 2002. Ésta se aplica según la importancia del edificio. Son considerados edificios de importancia especial diferentes tipos como hospitales, parques de bomberos, comunicaciones, transportes, o grandes centros comerciales.

4.3.4 Actuaciones prioritarias:

– Elaborar análisis nacionales de riesgos en función de escenarios posibles, teniendo en cuenta los fenómenos asociados. Estos escenarios deben ser multirriesgo y se utilizarán para mejorar la planificación de emergencias con intervención del Estado.

– Fortalecer los mecanismos administrativos y judiciales de control para vigilar el cumplimiento efectivo de los instrumentos preventivos, legales y técnicos sobre prevención en riesgo sísmico, especialmente el cumplimiento de la norma sismo resistente.

– Fomentar el desarrollo de estudios locales de riesgo sísmico, especialmente en las zonas más propensas a sufrir terremotos y el desarrollo de la planificación local especial ante este riesgo.

– Implantar un sistema de alerta e información preventiva ante el riesgo de tsunamis, así como desarrollar la planificación contemplada en la directriz básica de Protección civil ante el riesgo de maremotos.

4.4 Volcánicos.

4.4.1 Descripción: Aunque la España peninsular presenta evidencias geomorfológicas de un volcanismo geológicamente antiguo (Olot, Campo de Calatrava, Sierra de Gata), la Comunidad Autónoma de Canarias es la única que presenta una actividad volcánica muy reciente, que hace que sea el único ámbito territorial para el que la legislación vigente establece la necesidad de disponer de un Plan de Protección Civil ante dicho riesgo.

El archipiélago canario comprende siete islas volcánicas mayores que forman una cadena que se extiende unos 500 km a lo largo del Atlántico. Se dispone de registros históricos de erupciones en Tenerife, La Palma, El Hierro y Lanzarote. También se conocen erupciones volcánicas anteriores en Fuerteventura, por tanto, todas las islas mayores de Canarias, excepto La Gomera y Gran Canaria, tienen un volcanismo reciente activo.

La posibilidad de que se produzca una erupción volcánica varía dependiendo de la isla que se considere, pero en general es de moderada a baja, aunque para reducir su posible impacto, se debe prever la organización de los medios y recursos humanos y materiales, que pudieran ser requeridos para la protección y socorro de la población, en caso de que una erupción volcánica afectase a alguna de las islas.

Por otra parte el propio fenómeno volcánico puede manifestarse con múltiples fenómenos físicos peligrosos asociados, como sismicidad, caída de cenizas, coladas de lava o deslizamientos, entre otros, que no siempre cuentan con precursores detectables con la suficiente anticipación para poder adoptar las medidas de protección adecuadas.

4.4.2 Potenciadores:

– La incertidumbre ante la diversidad de fenómenos peligrosos que pueden manifestarse con una crisis volcánica.

– Los factores geográficos como la posición ultra periférica, la insularidad y la morfología del relieve de acusadas pendientes, que dificultan el transporte, conexión y movilización de los recursos existentes en las dos provincias canarias así como la aplicación de medidas de respuesta como pueda ser la evacuación llegado el caso.

– Los factores demográficos y socioeconómicos, caracterizados por el poblamiento disperso de la población autóctona y la concentración de población turística de orígenes culturales diversos.

– Finalmente, los largos periodos de inactividad volcánica, dificultan la adecuada percepción del riesgo en la población que pueda verse afectada.

CVE: BOD-2019-086-11386
Verificable en https://sede.defensa.gob.es/acceda/bod

4.4.3 Instrumentos normativos y de gestión.

– La directriz básica de protección civil ante el riesgo volcánico fue aprobada por Acuerdo del Consejo de Ministros del 19 de enero de 1996. En ella se consideran dos niveles de planificación: El estatal y el de Comunidad Autónoma, incluyendo en este último los planes de actuación que sean confeccionados por las entidades locales.

– El Plan Estatal ante el Riesgo Volcánico, aprobado por Acuerdo del Consejo de Ministros del 25 de enero de 2013 Se establece la organización y los procedimientos de actuación que permitan asegurar una respuesta eficaz.

– Real Decreto 953/2018, de 27 de julio, recoge en su artículo 15, las funciones y competencias encomendadas a la Dirección General del Instituto Geográfico Nacional (IGN), y en particular en el apartado d) establece como competencia del IGN la planificación y gestión de los sistemas de vigilancia y comunicación a las instituciones de la actividad volcánica en el territorio nacional y determinación de los peligros asociados.

– El Plan Especial ante Riesgo Volcánico de la Comunidad Autónoma de Canarias (PEVOLCA), aprobado el 30 de julio de 2018.

4.4.4 Actuaciones prioritarias.

– Impulsar la implantación de los Planes de Protección Civil a través de ejercicios y simulacros, así como con campañas de información a la población.

– Fomentar el desarrollo de escenarios posibles de riesgo, que permitan mejorar la planificación y el diseño de acciones a tomar, en función de su impacto

– Desarrollar las capacidades locales suficientes que posibiliten dar una respuesta inicial de manera eficaz a las posibles emergencias volcánicas.

– Elaborar análisis nacionales de riesgos en función de escenarios posibles, teniendo en cuenta los fenómenos asociados. Estos escenarios deben ser multirriesgo y se utilizarán para mejorar la planificación de emergencias con intervención del Estado.

4.5 Fenómenos meteorológicos adversos.

4.5.1 Descripción: Se considera fenómeno meteorológico adverso (FMA) a todo evento atmosférico capaz de producir, directa o indirectamente, daños a las personas y sus bienes o alterar la actividad humana de forma significativa.

Los fenómenos meteorológicos adversos producen graves daños personales y económicos, presentándose como los fenómenos que mayor número de víctimas mortales anuales ocasiona en España. Desde comienzos de siglo, alrededor del 83 % de las víctimas mortales en España por fenómenos naturales son debidos a fenómenos meteorológicos adversos, ya sea por causas directas o, más frecuentemente, por causas indirectas, al provocar el agravamiento de patologías previas.

Los fenómenos que habitualmente son los que producen mayor impacto en nuestro país son las tormentas, las olas de calor y los vientos fuertes, tanto en tierra como en línea de costa. Además, en los últimos años, también han afectado las tormentas extratropicales, en particular al archipiélago canario.

La sequía, consecuencia de la falta continuada de lluvia, afecta sistemáticamente al territorio ocasionando problemas socioeconómicos de diversa índole. Los efectos del cambio climático previsiblemente serán un aumento progresivo a lo largo del siglo XXI del número de días cálidos, una mayor duración de las olas de calor junto a una disminución en el número de días de helada y una disminución de los días de precipitación.

Las tormentas localmente cada vez más intensas y con características propias de otras latitudes también están afectando a nuestro territorio.

En España, los registros meteorológicos muestran un importante incremento de las temperaturas medias a lo largo del último medio siglo, más acentuado en la época estival. También se están batiendo los registros históricos de temperaturas máximas diarias, presentando una fuerte desestacionalidad. (42,6º C en mayo de 2015 en Valencia).

CVE: BOD-2019-086-11387
Verificable en https://sede.defensa.gob.es/acceda/bod

4.5.2 Potenciadores:

– Los efectos del cambio climático motivan que los fenómenos atmosféricos extremos habituales en nuestra geografía, sean cada vez más frecuentes e intensos incrementando su impacto en la sociedad.

– Los cambios de uso del suelo, el desarrollo urbano y de las infraestructuras del transporte, llevan aparejado el aumento de la impermeabilidad del suelo, que junto con la concentración de la población en núcleos urbanos en áreas costeras, son algunos de los elementos que aumentan la exposición y vulnerabilidad de la población.

4.5.3 Instrumentos normativos y de gestión:

– Plan Nacional de Predicción y Vigilancia de Fenómenos Meteorológicos Adversos: Meteo-alerta de la Agencia Estatal de Meteorología (AEMET).

– Plan Nacional de Actuaciones Preventivas de los efectos del exceso de temperaturas sobre la salud. Este plan pretende la prevención de daños sobre la salud provocados por el exceso de temperaturas. Existe una Comisión interministerial para su aplicación efectiva adscrita al Ministerio de Sanidad.

4.5.4 Actuaciones prioritarias:

– Elaborar la directriz básica ante el riesgo de FMA que fije los criterios y contenidos de la planificación de emergencias a nivel estatal y autonómico, y completar la planificación ante estos riesgos a nivel estatal y autonómico.

– Reforzar las capacidades de observación meteorológica con especial atención a las orientadas a la detección inmediata de la ocurrencia e intensidad de fenómenos meteorológicos adversos.

– Fomentar el desarrollo de investigaciones y estudios sobre los potenciales impactos de los fenómenos meteorológicos adversos (FMA) en la población, adecuando los sistemas que posibiliten su predicción y detección precoz, definir posibles acciones encaminadas a reducir la vulnerabilidad de la población y su adaptación a los fenómenos meteorológicos extremos.

– Contribuir a alcanzar una mayor implicación del conjunto de la sociedad y de los medios de comunicación en la respuesta integral y temprana de incidencias derivadas de fenómenos meteorológicos adversos.

4.6 Accidentes en instalaciones o procesos en los que se utilicen o almacenen sustancias peligrosas.

4.6.1 Descripción: Tras experimentar un importante incremento durante los primeros años del presente siglo, en los últimos cinco años el número de establecimientos donde se almacenan sustancias peligrosas y que han de estar acogidos a la Directiva 2012/18/UE se ha visto estabilizado, siendo actualmente de 899 en toda la geografía española.

En 2018 una cuarta parte de los establecimientos estaban dedicados al almacenamiento y distribución de hidrocarburos, otra cuarta parte se la repartían entre la fabricación e instalaciones de productos químicos y farmacéuticos, la producción, suministro y distribución de energía, y en menor cuantía la producción y almacenamiento de fertilizantes, pesticidas, biocidas y fungicidas. El resto de establecimientos se dedica a otro tipo de actividades industriales.

Geográficamente el mayor número de establecimientos se ubica en Cataluña seguido de Andalucía y Comunidad Valenciana.

Ese alto número de establecimientos contrasta con el relativo bajo número de accidentes que se suelen producir en los mismos, y que puede atribuirse a la mejora en las normativas que regulan dichos establecimientos. Atendiendo a los datos disponibles en la Dirección General de Protección Civil y Emergencias, en los últimos ocho años un 67 % de los accidentes solo han tenido repercusiones dentro del propio establecimiento mientras que otro 27 % además han podido tener víctimas y producir daños leves al exterior o medio

CVE: BOD-2019-086-11388
Verificable en https://sede.defensa.gob.es/acceda/bod

ambiente. En contraposición, solo se han producido tres accidentes de categoría 3 con víctimas y daños graves al exterior y medio ambiente.

En cuanto a las causas de los accidentes, la mitad se han producido por fallos en los sistemas mecánicos mientras que el resto se reparten por igual entre fallos operativos del personal y corrosión o fatiga de los componentes.

Como revelan algunos de los grandes accidentes relacionados con la industria química a lo largo de la historia –la tragedia de Seveso (Italia) en 1976, el desastre de Bhopal (India) en 1984, o la explosión de una refinería de BP en EEUU en 2005–, nos encontramos ante un riesgo con baja probabilidad de ocurrencia pero cuyas potenciales consecuencias pueden alcanzar niveles importantes.

4.6.2 Potenciadores:

– El primer potenciador global del riesgo de este tipo de instalaciones vendría determinado por unas condiciones socioeconómicas de crecimiento que llevan asociado un aumento en la producción y, por lo tanto, un crecimiento en el número de establecimientos.

– Analizando las causas de las emergencias que se han producido, dos factores importantes a tener en cuenta serían la falta de preparación adecuada del personal que ha de intervenir en las instalaciones, y la fatiga o deterioro de los materiales que componen las instalaciones.

4.6.3 Instrumentos normativos y de gestión:

– La Directiva 2012/18/UE del Parlamento Europeo y del Consejo relativa al control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas, que adopta el Sistema Global Armonizado de las Naciones Unidas de clasificación de sustancias.

– Real Decreto 840/2015, de 21 de septiembre, que coordina los procedimientos y las labores que han de desempeñar los industriales y las distintas autoridades competentes de la administración general y las comunidades autónomas, para la recopilación, intercambio y difusión de la información relativa a los establecimientos y sus inspecciones.

– Directriz Básica para el control y planificación ante el riesgo de accidentes graves que establece la estructura general de la planificación de protección civil ante este riesgo, que ha acogido el desarrollo de los Planes Especiales de Protección Civil en el ámbito autonómico y estatal.

4.6.4 Actuaciones prioritarias:

– Impulsar y mejorar la formación del personal encargado de las primeras intervenciones en caso de emergencia, incluyendo ejercicios y simulacros que ayuden a comprender los riesgos existentes y como atajarlo y mitigarlo.

– Potenciar el conocimiento por parte de la población de los riesgos y mecanismos de prevención y respuesta existentes, así como las medidas al respecto que puedan ser de su interés.

4.7 Transporte de mercancías peligrosas por carretera y ferrocarril.

4.7.1 Descripción: España es un país donde se produce un gran movimiento (en volumen y número de vehículos y trayectos) de mercancías peligrosas por ferrocarril y especialmente por carretera. La gran cantidad de establecimientos donde se almacenan sustancias peligrosas repartidos por toda la geografía peninsular (899 acogidos a la normativa Seveso), hacen especialmente relevante el flujo de sustancias entre las distintas industrias nacionales y de países vecinos (importaciones y exportaciones).

Según datos de los últimos mapas nacionales de flujos de mercancías peligrosas por carretera y ferrocarril de 2016, solamente en ferrocarril ese año se movieron alrededor de un millón y medio de toneladas de mercancías de este tipo. En cuanto al tránsito por carretera la información se recaba en base a estudios estadísticos que cifran dicho tránsito en unos 30 millones de toneladas.

CVE: BOD-2019-086-11389
Verificable en https://sede.defensa.gob.es/acceda/bod

Entre los productos más transportados figuran los líquidos inflamables (gasóleo y gasolinas principalmente) y los gases (como la mezcla de hidrocarburos gaseosos licuados), suponiendo más de la mitad del volumen transportado.

El accidente más grave registrado hasta la fecha en nuestro país, fue el ocurrido el 11 de julio de 1978, que arrasó el camping de Los Alfaques (Alcanar, Tarragona), por la explosión de un camión cisterna que transportaba propileno. El siniestro provocó 243 víctimas mortales y más de 300 heridos graves.

4.7.2 Potenciadores: De la información recabada en los últimos veinte años sobre las emergencias que se han producido en el T-MMPP, se puede constatar que la principal causa potenciadora del riesgo de estas emergencias son los accidentes convencionales de tráfico en los que se ven envueltos vehículos dedicados a este transporte, siendo los factores asociados a la propia mercancía (fallo en el contenedor o en la estiba) los menos numerosos.

Por ello se considera que los principales potenciadores de este riesgo se encuentran en la globalización, el crecimiento económico y un modelo productivo que intensifica el tráfico de estas mercancías.

4.7.3 Instrumentos normativos y de gestión:

– La Directiva 2008/68/CE del Parlamento Europeo y del Consejo sobre el transporte terrestre de mercancías peligrosas, que engloba el Acuerdo europeo sobre transporte internacional de MMPP por carretera (ADR) y el Reglamento relativo al transporte internacional de MMPP por ferrocarril (RID), ambos realizados por el Comité de Transportes Interiores de la UNCECE (Naciones Unidas).

– En el marco de la planificación de protección civil, se cuenta con una directriz básica de ámbito estatal y planes especiales de ámbito autonómico.

– Además se cuenta con distintas resoluciones legales anuales que establecen restricciones a la circulación estableciendo horarios y especificando carreteras por las que se permite la circulación, como la Red de Itinerarios de Mercancías Peligrosas por Carretera (RIMP).

4.7.4 Actuaciones prioritarias:

– Mejorar y potenciar los sistemas de información para conocimiento del riesgo. Para ello se hace necesario potenciar la colaboración de los actores directos implicados en la actividad para la recogida de toda esta información y elaboración de bases de datos, herramientas de análisis y estadísticas de emergencias que permitan elaborar mapas de flujos y riesgos.

– Mejorar y potenciar los sistemas de apoyo técnico a la gestión de las emergencias: Para ello se ha de potenciar la colaboración de los sectores implicados en la producción de las mercancías peligrosas (MMPP) con el aporte de información y medios para tratar las emergencias (Centro de Respuesta ante Emergencias-CERET).

– Impulsar la coordinación y colaboración entre la Administración General del Estado y las Administraciones autonómicas en los métodos de obtención y divulgación de los distintos sistemas de información.

– La mejora y actualización de la normativa en prevención y planificación de protección civil a raíz de la experiencia adquirida estos últimos años.

4.8 Riesgo nuclear y radiológico.

4.8.1 Descripción: En España, existen siete reactores nucleares en operación, ubicados en cinco emplazamientos, destinados a la producción de energía eléctrica, uno en cese definitivo de explotación y dos en fase de desmantelamiento.

Existen además cuatro instalaciones nucleares, distintas de las centrales nucleares, y 1.300 instalaciones radiactivas de distintas categorías, todas ellas reguladas, en las que manejan, procesan o almacenan sustancias radiactivas o nucleares.

En todas ellas podría existir un riesgo de liberación incontrolada o accidental de sustancias radiactivas al exterior, y en caso de producirse accidentes en estas instalaciones

CVE: BOD-2019-086-11390
Verificable en https://sede.defensa.gob.es/acceda/bod

podrían comportar un riesgo para la salud, tanto para el personal de tales instalaciones, como para el personal de intervención, la población del entorno, así como la contaminación del medio ambiente.

Además, hay infraestructuras como aeropuertos, puertos marítimos, aduanas y otras instalaciones y actividades no reguladas como las aquellas destinadas a la recuperación, almacenamiento o manipulación de materiales metálicos para su reciclado, en las que podría producirse algún incidente radiológico con posible repercusión en el exterior.

Por otro lado, no se pueden descartar los riesgos que puedan derivarse del uso inadecuado o negligente de las diversas fuentes de radiación.

4.8.2 Potenciadores: Si bien las principales causas de accidentes en estas instalaciones con repercusiones en el exterior son debidas a fallos técnicos o humanos, la experiencia ha puesto de manifiesto que hay sucesos externos como sismos, incendios e inundaciones y actos malintencionados que podrían originar incidentes en ellas.

Los principales potenciadores del riesgo estarían asociados a factores socioeconómicos y demográficos relacionados tanto con la distribución de la población en los entornos de las centrales nucleares, como al aumento de aplicaciones industriales relacionadas con sustancias peligrosas.

4.8.3 Instrumentos normativos y de gestión:

– A nivel internacional las recomendaciones de la Organización Internacional de Energía Atómica (OIEA) se encuentran recogidas en la normativa emitida por EURATOM en forma de directivas de la Unión Europea del mismo nombre. La más reciente de ellas referida a la gestión de estos riesgos es la directiva 2013/59/Euratom.

– Plan Básico de Emergencia Nuclear aprobado por Real Decreto 1546/2004, de 25 de junio.

– Plan de Emergencia Nuclear del Nivel Central de Respuesta y Apoyo, aprobado por Orden INT/1695/2005, de 27 de mayo.

– Planes de Emergencia Nuclear Exteriores a las Centrales Nucleares.

– Directriz Básica de planificación de protección civil ante el riesgo radiológico, aprobada por Real Decreto 1564/2010, de 19 de noviembre.

– Plan Estatal de Protección Civil ante el Riesgo Radiológico, aprobado por Real Decreto 1054/2015, de 20 de noviembre.

– Planes Especiales de Protección Civil ante el Riesgo Radiológico de comunidades autónomas.

4.8.4 Actuaciones prioritarias:

– Impulsar el desarrollo reglamentario con las modificaciones del Plan Básico de Emergencia Nuclear y la directriz básica protección civil ante el riesgo radiológico, así como avanzar en el proceso de planificación por parte de las comunidades autónomas frente al riesgo radiológico.

– Mejorar los mecanismos de coordinación entre las diferentes Administraciones, el Consejo de Seguridad Nuclear y los titulares de las instalaciones.

– Fortalecer las políticas de educación, información a los ciudadanos, y autoprotección, promoviendo una cultura preventiva.

– Impulsar la formación del personal de intervención adscrito a las organizaciones de respuesta y la realización de ejercicios y simulacros en el ámbito del riesgo nuclear.

CAPÍTULO 4

Misión, objetivo y líneas de acción de la Estrategia Nacional de Protección Civil

La misión o fin último de la protección civil, como instrumento de la política de seguridad pública, es proteger a las personas y bienes garantizando una respuesta adecuada ante los distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana, tomando en consideración la incidencia de los diferentes factores potenciadores de las amenazas y riesgos –en especial del cambio climático– y la necesidad de fortalecer la resiliencia comunitaria frente a este tipo de eventos.

CVE: BOD-2019-086-11391
Verificable en https://sede.defensa.gob.es/acceda/bod

En España, las políticas públicas de protección civil se articulan sobre la base de una acción concertada que involucre de forma eficiente todos los recursos necesarios de las distintas administraciones públicas, del sector privado así como la participación activa de los ciudadanos. Estas políticas están dirigidas al logro de unos objetivos compartidos que permitan la anticipación, prevención, respuesta eficaz y recuperación necesaria por los daños derivados de las amenazas y riesgos en el ámbito de la protección civil que se producen en España, y que pueden requerir de una acción concertada con otros actores internacionales.

La Estrategia de Seguridad Nacional de 2017 establece, junto con el resto de objetivos generales de la Seguridad Nacional, un objetivo estratégico prioritario en el ámbito de la protección civil: una consolidación del Sistema Nacional de Protección Civil como instrumento integrador de todas las capacidades de España para gestionar la respuesta ante emergencias y catástrofes que asegure su integración bajo el Sistema de Seguridad Nacional. Para la consecución de dicho objetivo se apuntaba hacia las siguientes líneas de acción estratégicas (LAE) para la Seguridad Nacional.

1. Implementar, a través de la colaboración entre todas las Administraciones competentes, la Estrategia Nacional de Protección Civil, tras su aprobación por el Consejo de Seguridad Nacional.

2. Completar el marco jurídico de la protección ante emergencias y catástrofes, desarrollando normativamente la Ley 17/2015.

3. Fomentar los mecanismos de colaboración y participación de la sociedad civil en las políticas públicas de protección civil, especialmente en materia de prevención.

4. Fortalecer la integración de capacidades de todo el Sistema Nacional de Protección Civil incrementando la cooperación y coordinación entre todas las Administraciones públicas competentes, con actuaciones concretas:

a) Constituir e implantar la Red de Alerta Nacional de Protección Civil para mejorar la prevención, con un enfoque integrado y multirriesgo.

b) Mantener directorios de capacidades.

c) Diseñar en común acciones de asistencia integral a las víctimas.

d) Establecer protocolos de gestión y comunicación a nivel nacional e internacional, en coordinación con la UE y otros organismos internacionales.

5. Promover la coordinación y cooperación internacional en materia de protección civil, con especial atención al mecanismo de protección civil de la UE y la Estrategia Internacional de Reducción del Riesgo de Desastres de la ONU, así como, de forma bilateral, con terceros países.

Teniendo en cuenta las anteriores LAE de la Estrategia de Seguridad Nacional, así como el análisis de los principales riesgos y amenazas que afectan a España en materia de protección civil, y que han quedado recogidas en el presente documento, los poderes públicos dispondrán los recursos humanos y materiales necesarios para desarrollar las siguientes líneas de acción de la Estrategia Nacional de Protección Civil:

– Impulsar el desarrollo normativo de la Ley 17/2015, promoviendo la elaboración de los correspondientes planes de protección civil, y en particular, la adopción de un Plan General Estatal de Protección Civil, que guarde la debida coherencia con las estrategias existentes para la adaptación al cambio climático.

– Fortalecer los vínculos entre los distintos planes de protección civil ante los diferentes tipos de riesgos y los instrumentos de planificación para la ordenación del territorio, uso del suelo y desarrollo urbanístico.

– Desarrollar e implementar las redes nacionales de información y alerta de protección civil.

– Mejorar las herramientas de coordinación entre las diferentes administraciones públicas, así como los mecanismos de participación y colaboración con ciudadanos, empresas y sociedad civil organizada.

CVE: BOD-2019-086-11392
Verificable en https://sede.defensa.gob.es/acceda/bod

– Renovar los instrumentos de recuperación postemergencia, con un enfoque basado en el fortalecimiento de una sociedad cada vez más resiliente frente a las emergencias y catástrofes.

– Mejorar la atención a las personas en situación de especial vulnerabilidad por razones sociales y/o personales, considerando esta variable tanto en la elaboración de los protocolos de actuación, como en la formación de los intervinientes y en los procedimientos de comunicación pública ante situaciones de emergencia.

– Impulsar la coordinación de las políticas de comunicación pública ante situaciones de emergencia o catástrofe, reforzando los canales y protocolos de comunicación ante este tipo de eventos.

– Fortalecer las políticas de educación, formación y autoprotección de los ciudadanos, promoviendo una cultura preventiva.

– Potenciar la cooperación internacional, y el desarrollo de actuaciones dirigidas a dar cumplimiento a los compromisos de España en el marco europeo y global, así como la participación en la acción exterior del Estado.

– Avanzar hacia la interoperabilidad de los centros de coordinación operativa y las capacidades de intervención a nivel nacional. Entre otras acciones, es preciso desarrollar el Plan Nacional de Interconexión previsto en la Ley 17/2015, y facilitar una formación básica común para los profesionales de las unidades de intervención de cualquier titularidad, con el fin de mejorar las posibilidades de una eficaz colaboración en la respuesta conjunta a las emergencias.

– Fomentar el desarrollo de nuevas herramientas predictivas de detección de materialización de riesgos naturales.

– Promover la realización de ejercicios y simulacros en el ámbito nacional e internacional.

CAPÍTULO 5

Seguimiento, evaluación y revisión de la Estrategia Nacional de Protección Civil

La Estrategia Nacional de Protección Civil será objeto de revisión, al menos, cada cinco años. También será revisada cuando así lo aconsejen las modificaciones de la Estrategia de Seguridad Nacional o las circunstancias cambiantes del entorno.

Un Comité Técnico de Seguimiento de la Estrategia Nacional de Protección Civil, presidido por el titular de la Subsecretaría del Interior y en el que estarán representados todos los departamentos ministeriales y organismos estatales que forman parte del Consejo Nacional de Protección Civil, llevará a cabo el seguimiento y evaluación del grado de desarrollo de los objetivos y líneas básicas de acción de la Estrategia Nacional de Protección Civil, pudiendo formular las correspondientes propuestas de revisión.

Este Comité Técnico de Seguimiento se reunirá, al menos, una vez al año y las funciones de secretaría del mismo serán asumidas por el secretario de la Comisión Permanente del Consejo Nacional de Protección Civil.

(B. 86-2)

(Del *BOE* número 103, de 30-4-2019.)

CVE: BOD-2019-086-11393
Verificable en https://sede.defensa.gob.es/acceda/bod

I. — DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

SEGURIDAD AÉREA

Orden PCI/489/2019, de 26 de abril, por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional.

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia de Seguridad Aeroespacial Nacional.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

Madrid, 26 de abril de 2019.–La Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, Carmen Calvo Poyato.

ANEXO

Estrategia de Seguridad Aeroespacial Nacional

Sumario

Resumen ejecutivo

La Estrategia de Seguridad Aeroespacial Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la seguridad del espacio aéreo y ultraterrestre, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

CVE: BOD-2019-086-11394
Verificable en https://sede.defensa.gob.es/acceda/bod

El documento se articula en cuatro capítulos. El primero, titulado «Visión integral de la Seguridad Aeroespacial», detalla aspectos generales de los sectores aéreo y espacial, describe brevemente su marco regulatorio, y justifica el uso de una única estrategia de seguridad aeroespacial para proteger los principales intereses nacionales en este ámbito.

El ámbito aeroespacial es tan importante para la moderna sociedad española que sin los servicios, aplicaciones y productos que proporciona, nos sería difícil imaginar su funcionamiento. Al mismo tiempo, el elevado uso de la tecnología y el altísimo nivel de interconectividad implican una especial vulnerabilidad ante las amenazas y desafíos, y una rápida velocidad de evolución de las crisis que afecten al ámbito.

El sector aéreo es uno de los elementos vertebradores del Estado español y un sector estratégico en la economía nacional. El sector está en crecimiento constante y actualmente se está desarrollando, de forma exponencial, el campo de las aeronaves no tripuladas que posibilitará el desarrollo económico en muchos sectores.

España tiene asignado un espacio aéreo de responsabilidad considerable que, desde el punto de vista de la defensa y la seguridad aérea nacional e internacional, es necesario proteger y para ello dispone de un potente sistema integrado en el de la OTAN para vigilar, controlar y dirigir, permanentemente (24/7), los medios de defensa oportunos. El Centro de Operaciones Aéreas Combinadas de Torrejón (CAOC-TJ) es la entidad desde donde se realiza la defensa aérea del flanco sur de la Alianza Atlántica (desde Turquía hasta las Islas Canarias) y desempeña un papel fundamental en la seguridad aeroespacial de España.

En el sector espacial, España es un miembro importante de varias organizaciones internacionales, participa en los principales proyectos europeos e internacionales, y acoge en su territorio importantes infraestructuras espaciales. En este sector, se está desarrollando actualmente la capacidad nacional de vigilancia y seguimiento espacial que permitirá contribuir a la elaboración de un catálogo de objetos espaciales en órbita.

La industria aeroespacial es muy importante para el país, tanto por su contribución al PIB nacional como por los numerosos puestos de trabajo altamente cualificados que aporta. Las capacidades únicas de nuestra industria aeroespacial y de defensa deben mantenerse y protegerse.

Desde el punto de vista de la seguridad, y dado que no existen límites físicos o funcionales entre los espacios aéreo y ultraterrestre, se considera que ambos forman un único ámbito, el aeroespacial, en el que las amenazas y desafíos se desarrollan a gran velocidad, lo que implica un tiempo de reacción muy corto y, consecuentemente, sean necesarias estructuras de decisión en tiempo casi real apoyadas en sistemas de mando y control que dispongan de buenas capacidades; que sean fiables; que estén perfectamente coordinados, tanto a nivel nacional como internacional; y que estén permanente disponibles.

En el aspecto normativo, los marcos legales de utilización del espacio aéreo y el ultraterrestre se basan en principios sustancialmente distintos; mientras que en el espacio aéreo rige el principio de soberanía nacional y uso flexible del espacio aéreo, el espacio ultraterrestre es considerado patrimonio común de toda la humanidad. Sin embargo, la regulación actual deja áreas de indefinición, como la delimitación del límite superior de la soberanía nacional del espacio aéreo, que en el futuro próximo puede ser una fuente de conflicto, al igual que el espacio ultraterrestre. Como muestra de ello, en el sector espacial han aparecido nuevos actores, como el denominado «Nuevo espacio», formado fundamentalmente por compañías privadas, que buscan nuevos modelos de negocio, tienen aspiraciones enfocadas más allá de la Tierra, y discuten, e incluso no aceptan, la capacidad normativa de los Estados sobre el espacio exterior.

El segundo capítulo «Amenazas y desafíos en el ámbito aeroespacial» define los conceptos de amenaza y desafío, y determina que las vulnerabilidades principales del ámbito aeroespacial derivan de su condición de espacio global común, de la elevada tecnificación de toda la infraestructura que opera y de la gran interconectividad, que posibilita los «efectos en cadena».

CVE: BOD-2019-086-11395
Verificable en https://sede.defensa.gob.es/acceda/bod

Las amenazas se agrupan en las seis áreas que define la Estrategia de Seguridad Nacional 2017: conflictos armados, terrorismo, crimen organizado, proliferación de armas de destrucción masiva, espionaje y ciberamenazas. Dentro de cada área se desarrollan las amenazas específicas para el ámbito aeroespacial como las incursiones no autorizadas; los secuestros de aeronaves, incluyendo la posibilidad de usar la propia aeronave como arma; el sabotaje de aeronaves e instalaciones; la perturbación de sistemas de comunicaciones, posicionamiento y vigilancia; las ciberamenazas; el uso del transporte aéreo para actividades del crimen organizado tales como el tráfico de mercancías ilegales, de personas, de animales, etc.; y el uso de aeronaves no tripuladas para cometer atentados terroristas o tráficos ilícitos. Sin embargo, las dos amenazas más importantes, por su capacidad destructiva y devastadora, son la utilización del instrumento aeroespacial en conflictos armados y la proliferación de armas de destrucción masiva.

Asimismo, los desafíos se agrupan en tres áreas: emergencias y catástrofes, epidemias y pandemias, y contaminación atmosférica y acústica; y dentro de cada una de ellas se desarrollan los desafíos específicos para el ámbito aeroespacial.

Dadas las características propias del ámbito aeroespacial, muchas de las amenazas y desafíos pueden producirse fuera de los espacios de soberanía y jurisdicción españoles, siendo necesario seleccionar la respuesta en función de las responsabilidades nacionales y de los compromisos internacionales contraídos por España.

El tercer capítulo «Objetivo, Principios y Líneas de Acción» aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a las cinco líneas de acción definidas en la misma para el ámbito aeroespacial, desarrollando medidas para cada una de ellas.

1. Fomentar una actuación coordinada de todas las Administraciones Públicas y departamentos con competencias en el espacio aéreo y ultraterrestre que permita establecer sinergias y abordar soluciones transversales.

Esta línea de acción se desarrolla mediante medidas en las áreas de coordinación, estructuras, formación y adiestramiento, y cultura de seguridad, para mejorar la toma de decisiones, la formación y adiestramiento avanzado del personal en gestión de crisis, la divulgación en la sociedad de la cultura de seguridad aeroespacial y las estructuras necesarias para llevar a cabo respuestas ágiles y adecuadas.

2. Fortalecer las capacidades de los organismos e instituciones nacionales, tanto públicos como privados, con competencias en estos ámbitos, para hacer frente a las diversas amenazas y desafíos propios del espacio aéreo y ultraterrestre.

Se desarrolla con medidas legales, de incremento y mejora de las capacidades de vigilancia, control y defensa del espacio aéreo, de vigilancia y seguimiento del espacio ultraterrestre, de supervivencia de infraestructuras críticas, de consolidación de la base industrial, de protección del medio ambiente, etc.

3. Perseverar en el análisis de riesgos y evaluación de medidas contra ciberataques, actos terroristas o delictivos u otros conflictos que afecten a las instalaciones aeroportuarias o al transporte aéreo, dentro o fuera del espacio aéreo español.

Se aborda esta línea de acción, con medidas en las áreas de ciberamenazas, terrorismo y desafíos, entre las que destacan el desarrollo de una política integral de ciberseguridad aeroespacial, la necesidad de canales específicos de distribución de inteligencia sobre amenazas específicas, y el incremento de capacidades del sistema español de seguimiento y vigilancia espacial.

4. Impulsar un desarrollo normativo del uso civil de aeronaves pilotadas remotamente que garantice el necesario equilibrio entre la seguridad de las personas, instalaciones y demás usuarios del espacio aéreo, y el desarrollo tecnológico y económico de un sector pujante de la economía española.

La regulación de los múltiples aspectos que implica la operación de aeronaves no tripuladas es condición indispensable para liberar el potencial del sector. La regulación

CVE: BOD-2019-086-11396
Verificable en https://sede.defensa.gob.es/acceda/bod

se desarrolla a nivel nacional e internacional, y es muy compleja porque hay que compatibilizarla con otras regulaciones que ocupan el mismo espacio. En el contexto de la seguridad aeroespacial, las medidas de tipo legal deben complementarse con la concienciación y sensibilización en su empleo, el desarrollo de capacidades contra aeronaves no tripuladas y su normativa de aplicación.

5. Apoyar el papel de España en el ámbito internacional, dentro del marco de compromisos y responsabilidades asumidos en materia de seguridad aérea y ultraterrestre.

Se sustancia con una serie de medidas de inversión, participación y representación, acuerdos bilaterales y multilaterales, mejora de la interoperabilidad, programas duales, coordinación meteorológica y de fenómenos de meteorología espacial, y coordinación para prevención de enfermedades contagiosas.

El cuarto capítulo «La Seguridad Aeroespacial en el Sistema de Seguridad Nacional» define la arquitectura orgánica de la seguridad aeroespacial. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Seguridad Aeroespacial que apoyará al Consejo de Seguridad Nacional y asistirá al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la seguridad aeroespacial, así como fomentando las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que actuará de forma complementaria al Consejo de Seguridad Nacional y, con el apoyo del Departamento de Seguridad Nacional, gestionará las situaciones de crisis del ámbito aeroespacial, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

CAPÍTULO 1

Visión integral de la Seguridad Aeroespacial

Aspectos generales del ámbito aeroespacial

El ámbito aeroespacial conecta todos los puntos de la Tierra y en él se desarrollan actividades tan fundamentales para la sociedad moderna que sería difícil concebir la vida actual sin ellas. Es transversal, facilita y potencia el crecimiento de todos los ámbitos, por lo que la interrupción o degradación de servicios aeroespaciales, por cualquier causa, tiene un potencial altamente disruptivo, con implicaciones en el normal desenvolvimiento económico y social de la nación, así como en su seguridad, pudiendo llegar a convertirse en un factor desestabilizante si se prolonga en el tiempo.

El ámbito crece de forma rápida y constante, y su valor se refleja en los servicios basados o posibilitados por las infraestructuras aeroespaciales en sectores tan relevantes como seguridad y defensa, meteorología, energía, telecomunicaciones, economía, transporte, marítimo, aviación, ingeniería, desarrollo urbano, ocio, turismo y otros muchos. Todos los sectores hacen un uso recurrente e intensivo de los servicios aeroespaciales para su normal funcionamiento.

La tecnología aeroespacial es un elemento indispensable en el funcionamiento de las sociedades modernas, sus activos forman parte de las infraestructuras críticas, y desempeña un papel crucial para cubrir las necesidades de los ciudadanos. Sin ella no hubiera sido posible llevar a cabo los avances que han posibilitado el desarrollo social actual. Su protección, y la de las infraestructuras que la albergan, son una prioridad para el funcionamiento y desarrollo de la sociedad.

El espacio aéreo y ultraterrestre es, al mismo tiempo, una fuente de oportunidades y de riesgos. Sus servicios deben ser protegidos de los desafíos y amenazas que puedan causar su interrupción o degradación, bien sea por causas naturales, meteorológicas, laborales o accidentes que por usos malintencionados o violentos como las

CVE: BOD-2019-086-11397
Verificable en https://sede.defensa.gob.es/acceda/bod

interferencias ilícitas (atentados, secuestro y sabotaje), la alteración de las señales emitidas en el espacio, el espionaje, las ciberamenazas, las acciones terroristas y los conflictos armados.

La Ley de Seguridad Nacional de 2015 incluye la seguridad del espacio aéreo y ultraterrestre entre los ámbitos de especial interés de la seguridad nacional, y la Estrategia de Seguridad Nacional de 2017 considera que en los espacios comunes globales (ciberespacio, espacio marítimo y espacio aéreo y ultraterrestre) cualquier disrupción puede suponer una rápida desconexión funcional e informativa y aconseja el desarrollo del mecanismo de gestión de crisis.

España, de acuerdo a sus capacidades y peso económico, es uno de los principales socios europeos del sector aeroespacial. Este sector es clave para el desarrollo económico y la seguridad de la nación y, consecuentemente, es fundamental garantizar un acceso adecuado a este ámbito, por lo que es necesario el desarrollo de una estrategia aeroespacial homogénea, desde la perspectiva genérica de la seguridad nacional, que permita alcanzar los objetivos marcados en la Estrategia de Seguridad Nacional vigente.

Aspectos generales del sector aéreo en España

España, por su especial distribución geográfica, tiene un área de responsabilidad aérea de un tamaño considerable (2.190.000 km^2) que representa un desafío de gran magnitud e implica un importante esfuerzo desde el punto de vista de los compromisos nacionales e internacionales: servicios de Control Aéreo, Búsqueda y Rescate, y Vigilancia Aérea relacionada con los flujos migratorios y las actividades ilícitas en el mar.

Para garantizar permanentemente la defensa del espacio aéreo nacional, España cuenta con el Mando de Defensa y Operaciones Aéreas. Cuenta con un potente sistema de mando y control que vigila, detecta, identifica, clasifica y, si es necesario, neutraliza, los objetos aéreos que penetran en el espacio aéreo de soberanía, responsabilidad o interés nacional y está enlazado y coordinado con el sistema de control y gestión civil del espacio aéreo de ENAIRE; a su vez, ambos sistemas están integrados respectivamente en los sistemas de defensa aérea de la OTAN y de gestión y control del espacio aéreo europeo (EUROCONTROL).

En el dominio de la aviación civil, el transporte aéreo es un elemento vertebrador del Estado y uno de los sectores estratégicos de la economía nacional. La disposición del territorio nacional con la península, los archipiélagos Canario y Balear, y las ciudades autónomas de Ceuta y Melilla, así como su situación entre los continentes europeo y africano, y su orientación abierta al océano Atlántico y mar Mediterráneo, le confieren considerables ventajas para convertirse en un auténtico nodo del transporte aéreo intercontinental (Europa-África-América).

Las cifras del transporte aéreo, en crecimiento constante los últimos años, significan la importancia del mismo para la economía nacional: 266 millones de pasajeros; 690 compañías aéreas, que operan en el país y unen 48 aeropuertos con 350 destinos diferentes en más de 140 países; 36 compañías españolas que movieron 88 millones de pasajeros; 2,3 millones de operaciones; 1,1 millones de Tm de carga. El gestor aeroportuario español (AENA), cuya propiedad mayoritaria corresponde al Estado, es el mayor gestor mundial de infraestructuras aeroportuarias.

La contribución directa del sector aeronáutico español (transporte aéreo, aeropuertos, navegación aérea e industria aeronáutica) supone un 2,5% del PIB nacional y genera más de 100.000 empleos directos de alto valor añadido debido a su estabilidad, calidad y alta cualificación. El sector aeronáutico transporta al 80% de los turistas que eligen nuestro país; y el turismo, que es nuestra primera industria nacional, aporta el 15% del PIB y da trabajo a casi tres millones de personas.

La industria aeronáutica española se encuentra entre las primeras potencias mundiales con empresas de primera línea y presencia internacional. La fortaleza de la base industrial aeroespacial nos permite disponer de la capacidad de controlar todo el

CVE: BOD-2019-086-11398
Verificable en https://sede.defensa.gob.es/acceda/bod

ciclo de vida (diseño, desarrollo, producción, soporte) de una aeronave completa, integrar aviones y sistemas, ser líderes en el desarrollo y bienes de equipo para la fabricación de composites para aeronaves, y disponer de empresas auxiliares de muy alta capacitación tecnológica.

En el área de aeronaves no tripuladas, el crecimiento del sector ha sido exponencial y la Agencia Estatal de Seguridad Aérea (AESA) ya tiene registrados más de 3600 operadores, 4600 pilotos y 5400 aeronaves. La entrada en vigor del RD 1036/2017 ha ampliado el número de escenarios en los que poder realizar operaciones aéreas con aeronaves tripuladas remotamente y ha posibilitado un desarrollo económico en sectores como la agricultura, energía, cine, fotografía y vídeo, levantamientos aéreos (topografía y fotogrametría), construcción, minería, etc. Esta nueva normativa ha representado un fuerte impulso para el desarrollo del sector, mejorando nuestra competitividad, fomentando la creación de empleo de alta cualificación y disminuyendo el impacto ambiental.

Aspectos generales del sector espacial en España

España es un país con un alto uso y dependencia de los sistemas espaciales, y dispone de capacidades espaciales propias en telecomunicaciones, observación de la tierra, meteorología, teledetección y, vigilancia y seguimiento espacial. Además, como Estado miembro de la UE, tiene acceso a la utilización de las capacidades desarrolladas por los programas espaciales de la UE.

España es miembro de varias organizaciones internacionales con actividades espaciales como la Agencia Europea del Espacio, EUMETSAT (la organización europea para la explotación de satélites meteorológicos y estudio del clima), la Agencia Europea de Defensa, la UE, la OTAN y la ONU. Participa en los principales proyectos internacionales y europeos del sector espacial, y aloja en su territorio importantes infraestructuras espaciales nacionales e internacionales.

La gestión de la política espacial por parte de la administración española, la coordinación y colaboración de los departamentos ministeriales se regula mediante comités de coordinación: el Comité Interministerial de Sistemas Globales de Navegación por Satélite, el Comité Director del Programa Nacional de Observación de la Tierra, la Comisión Interministerial de política industrial y tecnológica del espacio, y la Comisión de Seguimiento Interministerial de Sistemas de Vigilancia y Seguimiento Espacial.

El país cuenta en la actualidad con un extenso catálogo de medios espaciales en forma de infraestructuras, centros de investigación, tejido industrial y sistemas espaciales en funcionamiento, que nos sitúan entre los principales actores del sector espacial internacional. Con estos medios se atienden necesidades de organizaciones públicas, privadas y de los ciudadanos, y también aquellas relacionadas con la defensa y la seguridad. Disponemos de sistemas de comunicaciones seguras, sistemas de observación de la Tierra, sistemas de posicionamiento por satélite… gracias al esfuerzo creciente y continuado del sector, respaldado por la inversión proveniente, en su mayor parte, de las administraciones públicas.

En el área de los Sistemas Globales de Navegación por Satélite, Galileo y EGNOS (sistema de aumento de precisión e integridad de la señal de la constelación de satélites GPS y Galileo) constituyen la solución de la UE para sistemas de posicionamiento y la única infraestructura íntegramente de su propiedad. La UE estima que en el futuro el 11% del PIB de la UE dependerá de los sistemas de posicionamiento debido al creciente número de aplicaciones que utilizan su señal.

Actualmente se está desarrollando la capacidad nacional de vigilancia y seguimiento espacial, que permite el seguimiento de reentradas atmosféricas, el estudio de fragmentaciones, la prevención de colisiones y el apoyo a los lanzamientos hacia el espacio. Para ello, se ha impulsado el Programa de Vigilancia y Seguimiento Espacial español, dentro de las contribuciones nacionales para la Agencia Europea del Espacio.

CVE: BOD-2019-086-11399
Verificable en https://sede.defensa.gob.es/acceda/bod

Esta capacidad posiciona a España entre las pocas naciones con posibilidad de contribuir a la elaboración de los imprescindibles catálogos de objetos espaciales en órbita, gracias a la combinación de sistemas ópticos y radáricos, adecuadamente integrados en un centro de operaciones. De esta forma, España se encuentra preparada para participar en futuras iniciativas de mutualización de capacidades de vigilancia, seguimiento y control en el espacio ultraterrestre. Adicionalmente, esta capacidad prepara a la nación para avanzar en el campo de la seguridad aeroespacial ante la posibilidad de que, en un futuro próximo, el espacio se convierta en un área de enfrentamiento entre las grandes potencias, EE.UU., Rusia y China, que actualmente compiten por el liderazgo mundial en el espacio.

La industria espacial española dispone de amplias capacidades en todos los segmentos (vuelo, tierra, lanzadores) que van desde la fabricación de equipos hasta la integración de sistemas complejos (satélites, centros de operaciones, etc.); también tiene presencia en el sector de aplicaciones y servicios, con varios operadores de satélites. El sector emplea alrededor de 3.500 personas, con un altísimo porcentaje de trabajadores de alta cualificación.

El espacio es rentable para la nación, para la sociedad y para la industria: es un depósito de conocimiento, permite importantes aplicaciones que mejoran la calidad de vida de los ciudadanos, posee implicaciones relevantes en materia de seguridad y es una fuente de creación de empleo de alta cualificación. La demanda de servicios de satélites continuará incrementándose y el Estado apoyará al sector para disponer de la mayor autonomía posible, reduciendo la dependencia de otras potencias en el suministro de servicios fundamentales para el funcionamiento y la economía del país.

El espacio proporciona discreción y libertad de acción, está débilmente regulado, excepto en materia de comunicaciones, tiene un potencial económico enorme y la creciente facilidad de acceso introduce nuevos actores, estatales y no estatales (organizaciones, empresas, individuos…), que compiten por los recursos. Eso lo convierte en un foco potencial de disputas, amenazas y desafíos que las naciones deberán afrontar individual y colectivamente.

Marco regulatorio en el ámbito aeroespacial

Las reglas de utilización del espacio aéreo y del espacio ultraterrestre se fundamentan en principios sustancialmente distintos: mientras que el principio de soberanía estatal rige sobre el espacio aéreo nacional, el espacio ultraterrestre es considerado como patrimonio común de toda la humanidad; esto se explica por el distinto momento histórico en que se han ido desarrollando las actividades en uno y otro, y la percepción de la amenaza que representaban.

El espacio aéreo dispone de un marco legislativo muy ligado a la progresiva tecnificación de los medios de transporte aéreo, y que funcionalmente atiende a los ámbitos de la seguridad operacional, la protección de la aviación civil frente a actos de interferencia ilícita, y otros aspectos, principalmente comerciales y económicos, calidad, derechos del pasajero, y medioambientales. La Organización de Aviación Civil Internacional (OACI), agencia especializada de Naciones Unidas, es la fuente primaria de normativa de la que derivan la mayoría de las normas de los 192 Estados que actualmente forman parte de la Organización; una buena parte de la normativa OACI se incorpora directamente a nuestro ordenamiento jurídico, a través de Reglamentos o Directivas de la UE.

La seguridad aeroespacial nacional se basa en una serie de normas esenciales: la Ley 5/2005 de Defensa Nacional, la Ley 36/2015 de Seguridad Nacional, la Ley 8/2011 por la que establecen medidas para la protección de infraestructuras críticas, la Ley 21/2003 de Seguridad Aérea y la Ley 48/1960 de Navegación Aérea. En lo que respecta al ámbito de la aviación civil, los organismos que se ocupan de la seguridad son el Comité Nacional de Seguridad para la Aviación Civil creado por RD 550/2006, y la Agencia Estatal de Seguridad Aérea, creada por RD 184/2008.

CVE: BOD-2019-086-11400
Verificable en https://sede.defensa.gob.es/acceda/bod

La Ley 48/1960 de Navegación Aérea, que está en parte derogada o superada por otras normas, sigue siendo una referencia básica a la hora de configurar el entorno jurídico del espacio aéreo español. En lo que respecta al espacio aéreo de soberanía, la Ley define con claridad su delimitación horizontal, pero no la vertical, ya que no existe un acuerdo internacional sobre el límite del espacio ultraterrestre a partir del cual la soberanía del Estado subyacente deja de ser efectiva. Esta laguna legal cobra mayor importancia con los actuales avances tecnológicos y la carrera espacial, y está pendiente de resolución por la comunidad internacional.

En el sector de las aeronaves no tripuladas, la normativa nacional (RD 1036/2017) regula, en el espacio aéreo de soberanía nacional, la utilización civil de las aeronaves pilotadas por control remoto cuyo peso sea menor de 150 Kg, posibilitando el desarrollo del sector y garantizando la seguridad de las operaciones. El enorme desarrollo previsto en este sector exige completar la regulación, a nivel nacional e internacional, de la operación de aeronaves no tripuladas en todo el espacio aéreo, lo cual representa un enorme reto técnico y de seguridad.

En el espacio, la ausencia de derechos de soberanía y la libertad de exploración en condiciones de igualdad explican la naturaleza de los instrumentos internacionales que regulan su utilización. Uno de los grandes retos que presenta el ámbito espacial, por su condición de espacio global, es la dificultad de dotarle de un marco regulatorio aceptado y ratificado por todas las naciones.

La Guerra Fría trajo la regulación de las actividades en el ámbito espacial y las Naciones Unidas impulsaron una serie de tratados, acuerdos, convenios, principios y resoluciones conexas que se encuentran actualmente en diferentes estados de ratificación, firma y aceptación de derechos y obligaciones, sin que ninguno, a excepción del de la Unión Internacional de Telecomunicaciones, esté ratificado por todos los países.

Los tratados más importantes como el Tratado del Espacio de 1967, que constituye la piedra angular de la gobernanza del espacio exterior, y el de la «Prohibición de realizar ensayos nucleares en la atmósfera, el espacio ultraterrestre o submarinos», de 1963, también han sido ratificados por las principales potencias.

Todas estas normas se hicieron antes de 1983, cuando la percepción de los satélites era de objetos cuya tecnología y coste sólo estaba al alcance de los Estados más poderosos. Hoy en día, el aprovechamiento de componentes estándares comerciales, para reducir los costes de producción y el tiempo de desarrollo, ha proporcionado una facilidad de acceso al espacio que ha cambiado esa visión y ha dado lugar al denominado «Nuevo Espacio» en el que las compañías privadas, fundamentalmente, irrumpen con nuevas tecnologías, ideas de gestión y competitividad, para crear un nuevo modelo de negocio con aspiraciones enfocadas más allá de la Tierra, donde realizar actividades de todo tipo que van desde la operación de pequeños satélites en órbitas bajas, hasta la minería en el espacio exterior, la recogida de basura espacial y la colonización de otros planetas. Se estima que su crecimiento será exponencial en los próximos años, dadas su efectividad, fiabilidad y rentabilidad.

Los acuerdos que España ha ratificado en las Naciones Unidas, determinan que el Estado es responsable subsidiario de las actividades espaciales que puedan hacer sus nacionales (personas, entidades públicas o empresas) y en consecuencia se ha identificado la necesidad de regular las actividades espaciales que puedan llevar a cabo operadores no estatales.

Con la creciente facilidad de acceso al espacio se produce una mayor competencia, particularmente en la asignación y utilización de órbitas y de frecuencias de radio. En este entorno, la necesidad de regulación se vuelve necesariamente mayor y pone a prueba la eficacia del marco jurídico internacional. En consecuencia, varios países ya están tomando medidas para proteger sus activos en el espacio o para denegar su acceso a otros actores; tal es la criticidad de asegurar su acceso, que el espacio está comenzando a vislumbrarse como un futuro escenario de conflicto.

CVE: BOD-2019-086-11401
Verificable en https://sede.defensa.gob.es/acceda/bod

Dos espacios, una Estrategia de Seguridad

El espacio aéreo y el ultraterrestre, no son elementos separados ni desde el punto de vista físico, ni funcional. Desde el punto de vista físico, no es posible establecer límites entre ellos claramente definidos, pues presentan una clara continuidad física y no hay un punto evidente donde acaba uno y empieza otro, al no existir barreras naturales que los delimiten.

El espacio aéreo y el ultraterrestre están altamente tecnificados, en continua evolución, y con un gran potencial de desarrollo. Desde el punto de vista del empleo del espectro electromagnético ambos se comportan como un único medio cuyas capacidades, en su desarrollo, son además completamente dependientes del Ciberespacio.

Desde un punto de vista legal, en los tratados internacionales hay una falta de definiciones ampliamente aceptadas sobre la delimitación vertical entre el espacio aéreo y el espacio ultraterrestre y, por tanto, no hay una altitud que determine claramente cuál es el espacio aéreo de soberanía de un país. El tráfico aéreo civil actual tiene como límite práctico actual los 18 km de altitud y los satélites normalmente operan por encima de los 160 km de altitud, pero la evolución de la tecnología está contribuyendo a que esa «franja intermedia» se utilice crecientemente con fines científicos, comerciales y militares, sin que por el momento haya ninguna regulación en vigor aunque la Organización de Aviación Civil Internacional (OACI) y diversos organismos europeos, están estudiando las operaciones en el «espacio aéreo de gran altitud» y la transición al espacio aéreo desde la zona orbital y suborbital.

Desde el punto de vista de la seguridad, se debe tener presente que todo objeto que pueda alcanzar la superficie de la Tierra proveniente del espacio ultraterrestre y que pueda constituir una amenaza o un desafío, ineludiblemente tendrá que transitar por la «franja intermedia» y por el espacio aéreo, lo que hace necesario extender las funciones de vigilancia, detección, identificación y clasificación de dichos objetos para decidir la respuesta adecuada. Muchos de los sistemas empleados actualmente para vigilancia y control aéreo se utilizan también para la vigilancia espacial y cada día prestan más atención a esa «franja intermedia» de la atmósfera.

Es importante recordar que el espacio aéreo está compartido por un elevado número de agentes, en ocasiones con intereses diferenciados, como las compañías aéreas, la aviación militar, la privada y la deportiva, los trabajos aéreos, y en los últimos tiempos, también las aeronaves tripuladas remotamente, que presentan un gran potencial de crecimiento y también de riesgos y amenazas.

La inmediatez que caracteriza generalmente a las amenazas y desafíos aeroespaciales, implica que los sistemas de mando y control aeroespaciales deban estar permanentemente activados (24/7), coordinados, y dotados de los elementos de monitorización de la situación y de las estructuras de decisión, en tiempo casi real, que posibiliten la necesaria anticipación y rapidez en la respuesta.

El espacio aéreo y el ultraterrestre se configuran en definitiva como un espacio unificado y continuo, verdadero elemento sustantivo en el que se desarrolla toda esta actividad, sometido a amenazas y desafíos comunes, y con una interdependencia funcional absoluta. Su seguridad se contempla de forma unificada y coherente, como lo es su propia naturaleza, a través de una estrategia de seguridad aeroespacial que los trata como un ámbito único, permitiendo incrementar la eficacia de las medidas a aplicar en la vigilancia, control e intervención de actividades, tanto aéreas como espaciales, por parte de las autoridades responsables.

Intereses nacionales a proteger

El secuestro aéreo que se produjo en 2001 para atentar contra las Torres Gemelas en Nueva York y el Pentágono, demostró que una aeronave civil podía ser utilizada como un arma con un alto poder destructivo contra edificios o instalaciones de cualquier tipo, causar miles de víctimas y generar un estado de terror en la sociedad. El secuestro de

CVE: BOD-2019-086-11402
Verificable en https://sede.defensa.gob.es/acceda/bod

una aeronave de la compañía Germanwings en 2015 por un miembro de la tripulación con el objetivo de suicidarse, terminó con el asesinato de las 149 personas que iban a bordo cuando estrelló el aparato contra los Alpes franceses.

Incidentes como los mencionados parecían improbables hasta que sucedieron. La imaginación para causar daños, muerte y destrucción, sembrar el pánico y el terror por cualquier causa racional o irracional, no parece tener límites y, desafortunadamente, hoy en día hay muchos medios disponibles para hacerlo.

Todo ello nos lleva a identificar los principales intereses nacionales objeto de protección ante los desafíos y amenazas del ámbito aeroespacial; son los siguientes:

– La vida de los españoles, su seguridad, bienestar e intimidad en la Tierra, aire o espacio;
– El cumplimiento de la legislación nacional e internacional en el ámbito aeroespacial;
– La libertad de navegación aérea y la seguridad de las aeronaves que transitan por el espacio aéreo de responsabilidad nacional;
– El espacio aéreo de soberanía, responsabilidad o interés nacionales, frente a las incursiones no autorizadas de cualquier tipo;
– El libre acceso y explotación segura del espacio;
– Las infraestructuras, medios y servicios aeroespaciales de alto valor ante los desafíos y amenazas procedentes tanto del aire-espacio como de otros ámbitos;
– Las capacidades de la industria aeroespacial nacional;
– La salud de la sociedad ante la propagación intencionada o inintencionada, de agentes patógenos o sustancias tóxicas por medios aeroespaciales;
– El medio ambiente aeroespacial.

CAPÍTULO 2

Amenazas y desafíos en el ámbito aeroespacial

Introducción al concepto de amenaza y desafío en el ámbito aeroespacial

La Estrategia de Seguridad Nacional de 2017 contempla un catálogo general de amenazas y desafíos para la Seguridad Nacional que es necesario particularizar al ámbito aeroespacial.

Las amenazas a considerar son todas aquellas que comprometen o pueden socavar la Seguridad Nacional, entendiendo por amenaza un potencial daño, fruto de un acto deliberado y de naturaleza delictiva o ilícita. Entre ellas, por sus potenciales efectos sobre la Seguridad Nacional, destacan aquellas que puedan afectar al conjunto de infraestructuras con impacto en sectores estratégicos tales como la defensa, la energía, los flujos de información financiera o el normal funcionamiento de determinados servicios básicos para la sociedad.

Los desafíos no tienen intencionalidad, pero pueden provocar situaciones de inestabilidad o propiciar el surgimiento de amenazas, agravarlas o acelerar su materialización. La Estrategia de Seguridad Nacional 2017 contempla las emergencias y catástrofes, las epidemias y pandemias, y los efectos derivados del cambio climático como factores con un potencial impacto sobre la seguridad aeroespacial.

El ámbito aeroespacial posee una serie de características diferenciadoras que potencian su vulnerabilidad. Estas serían su condición intrínseca de espacio global común, la elevada tecnificación de la práctica totalidad de la infraestructura que en él opera y la alta posibilidad de efectos en cadena derivados de la gran interconectividad.

Las amenazas y desafíos en el ámbito aeroespacial pueden producirse en los espacios de soberanía y jurisdicción aérea españoles, así como fuera de estos; en ambos casos la respuesta se arbitraría en función de las responsabilidades nacionales y de los compromisos internacionales contraídos por España.

CVE: BOD-2019-086-11403
Verificable en https://sede.defensa.gob.es/acceda/bod

De forma genérica, las incursiones no autorizadas constituyen la amenaza más obvia que podría desarrollarse en el espacio aéreo. Estas incursiones tomarán la forma de amenaza cuando se trate de actos deliberados provocados por la acción humana, como es el caso del secuestro de aeronaves con fines terroristas, el sobrevuelo de misiles balísticos, los vuelos suborbitales y pseudo-satélites no autorizados sobre el territorio de soberanía nacional, las incursiones de aeronaves militares y civiles no autorizadas, las aeronaves no tripuladas con fines de inteligencia, las aeronaves utilizadas para contrabando o paso ilegal de fronteras, los ingenios con elementos de perturbación electromagnética, etc.

Entre las incursiones no autorizadas hay que considerar las ciberamenazas que intentan explotar las vulnerabilidades de los sistemas informáticos y las telecomunicaciones del ámbito aeroespacial. Estas resultarían especialmente críticas en caso de afectar a la navegación, los sistemas de control aéreo, los sistemas de control embarcados en las aeronaves, las comunicaciones, la meteorología, la observación de la Tierra, etc. En este ámbito, el potencial disruptivo es muy grande porque al estar altamente tecnificado y sincronizado, los efectos se harían sentir de forma inmediata.

En el ámbito aeroespacial, las amenazas evolucionan con la misma rapidez que la tecnología y el riesgo es no disponer de los medios y la organización necesarios para hacerles frente y poder reaccionar a tiempo.

Los desafíos en el ámbito aeroespacial provienen principalmente de fenómenos y catástrofes no intencionados como la caída de meteoritos; la basura espacial incontrolada; las erupciones volcánicas; los terremotos; los fenómenos atmosféricos severos; los fenómenos de meteorología espacial; los accidentes; las emergencias; y las epidemias y pandemias, que pueden distribuirse por medios aeroespaciales y extenderse a humanos, animales y vegetales.

Amenazas

Conflictos Armados

El empleo del instrumento aeroespacial tiene un impacto decisivo en el resultado de los conflictos armados y constituye una de las amenazas más letales a la que se puede enfrentar un Estado, ya que tiene la capacidad de actuar de forma precisa, contundente, rápida y en profundidad, contra los centros de gravedad, es decir, contra los intereses vitales y estratégicos de la nación.

Los medios aeroespaciales tienen una gran versatilidad, permitiendo adecuar o modular la intensidad de la respuesta a la naturaleza de la amenaza. Su alta disponibilidad y velocidad les convierte en una de las más rápidas opciones de respuesta y su forma de actuar permite reducir el impacto mediático y político, al no necesitar ocupar el terreno del adversario.

Entre los elementos principales del instrumento aeroespacial destacan los sistemas de vigilancia y control, pues son los «ojos» mediante los cuales es posible detectar e identificar las amenazas que se desarrollan en el ámbito aeroespacial y dirigir los medios de defensa oportunos (aeronaves, misiles superficie/aire en tierra o embarcados…) para hacerles frente. Por otra parte, los sistemas de control del tránsito aéreo civil mantienen un flujo seguro y ordenado del tráfico aéreo, contribuyendo a la identificación de los medios aéreos hostiles y, en su caso, al control y neutralización de los mismos.

En consecuencia, tanto la protección física, electromagnética y cibernética de los sistemas de vigilancia y control, militares y civiles, como la capacidad para afectar a los medios correspondientes de un potencial adversario, son una prioridad para el instrumento aeroespacial.

Una de las áreas en las que se ha experimentado una mayor evolución, es en el desarrollo de capacidades que impiden el acceso de las fuerzas propias a determinadas áreas o dominios en disputa, debido principalmente a la mejora sustancial de las capacidades de defensa aérea, y al incremento del alcance y tecnología de los misiles aire-aire, tierra-aire y tierra-tierra, lo que limita enormemente la autonomía estratégica de

CVE: BOD-2019-086-11404
Verificable en https://sede.defensa.gob.es/acceda/bod

la que hasta ahora habían disfrutado los países de la OTAN y la UE en sus operaciones en el ámbito aeroespacial, y les obliga a desarrollar nuevas capacidades para hacerles frente.

Debido a la posibilidad creciente de que determinados actores estatales y no estatales accedan a la tecnología necesaria para su desarrollo, los misiles balísticos e hipersónicos constituyen una de las amenazas que más preocupa a la comunidad internacional. Combatir esta amenaza requiere de importantes capacidades en inteligencia, así como medios para detectarla, y una capacidad de mando y control que permita establecer actuaciones para combatirla de una forma eficaz, con medios adecuados, tanto de forma autónoma como en colaboración con socios y aliados.

Los satélites pueden verse amenazados en caso de conflicto. Cada día se incrementa la probabilidad de que la mayor parte de las naciones, e incluso organizaciones terroristas o criminales, dispongan en el corto-medio plazo de capacidades para neutralizar un satélite. Los países que disponen de la capacidad para lanzar un ataque letal sobre los activos en órbita, no es probable que lo realicen por el riesgo de dañar a los propios sistemas que provocaría la destrucción del aparato enemigo, si este desencadenase una reacción en cadena producida por la nube de desechos espaciales. Sí que es concebible, la neutralización e inutilización de sistemas espaciales por otros medios, fundamentalmente, infiltrándose en sus sistemas de control en tierra con el objetivo de suplantar a sus legítimos operadores o, simplemente, de inutilizarlos mediante sistemas de energía dirigida, perturbación electromagnética y ciberataques.

Cualquier ataque a los satélites, de los que la sociedad española depende para obtener servicios esenciales (comunicaciones, información meteorológica, navegación, etc.), tendría enormes consecuencias económicas, sociales y de seguridad.

Considerando todo lo anterior, las amenazas principales en el ámbito aeroespacial, en caso de conflicto armado, son las capacidades aeroespaciales del adversario, que incluyen, entre otros:

– El armamento aire-aire y aire-tierra, y sus vectores lanzadores.
– Los misiles balísticos y de crucero, incluidos los hipersónicos.
– Las armas de energía radiada.
– Los dispositivos disruptores de servicios esenciales (comunicaciones, navegación, control, servicios de posicionamiento, meteorología…).
– Los satélites y medios anti-satélite.
– Los mecanismos de captura de sistemas aeroespaciales.
– Los ciberataques.

Terrorismo

Las organizaciones terroristas siempre han tenido al sector aéreo, principalmente la aviación comercial (aeronaves y aeropuertos), entre sus objetivos de primer nivel por la facilidad de conseguir un alto número de víctimas, la repercusión mediática y el impacto económico inmediato. Estas organizaciones mantienen la presión sobre el sector aprovechando las múltiples posibilidades que ofrece la evolución tecnológica, lo que genera una preocupación constante para mantener unos adecuados niveles de seguridad e implica un esfuerzo económico que afecta significativamente a las economías de los países.

Las principales amenazas al sector aeroespacial son las siguientes:

– El secuestro de aeronaves, acto ilícito por el que una persona o un grupo de personas se apoderan de una aeronave. La finalidad del secuestro va desde la utilización de los pasajeros rehenes para algún tipo de negociación hasta la de utilizar la aeronave como arma; esta amenaza, que se materializó por primera vez en los ataques terroristas del 11S, se denomina Renegade.

CVE: BOD-2019-086-11405
Verificable en https://sede.defensa.gob.es/acceda/bod

– El sabotaje aéreo, acto intencionado que tiene como objetivo la destrucción o incapacitación de aeronaves, infraestructuras aeroportuarias y aeroespaciales, sistemas de navegación, comunicación y posicionamiento, y servicios aeronáuticos.

– El ataque a una aeronave en vuelo utilizando armamento terrestre (Sistemas de defensa aérea portátiles, armamento ligero, armas antiaéreas, etc.), e incluso, armas de energía radiada.

– El uso de dispositivos, como el láser, con el propósito de deslumbrar o cegar a pilotos, y más raramente a controladores, constituye una amenaza potencial creciente que puede llegar a tener consecuencias catastróficas.

– Empleo de aeronaves ligeras para la comisión de atentados terroristas.

– Empleo de aeronaves no tripuladas con el objetivo de provocar un incidente/accidente aéreo, utilizándolas directamente como armas, como elementos disruptores de la actividad aérea, o liberando con ellas armamento, explosivos, sustancias nocivas...

– Ciberataques.

– La captación y radicalización ideológica dirigidas a personal vinculado con el entorno aéreo: tripulaciones, controladores aéreos y trabajadores de aeropuertos, para inducirles a participar, planear y cometer actos terroristas.

Además, el terrorismo tiene otros objetivos en los que puede utilizar elementos aeroespaciales o tecnológicos para cometer atentados.

– Las aeronaves no tripuladas, son el elemento aéreo más recientemente incorporado al arsenal terrorista. La facilidad de adquisición y manejo de estas plataformas, su relativo bajo coste, la dificultad de controlar su operación, y sus múltiples posibilidades de empleo, sólo limitadas por la imaginación terrorista, las convierten en candidatas ideales para ser empleadas por el terrorismo. La ausencia de una base reguladora integral en su producción y comercialización facilita su uso para fines ilícitos.

– La perturbación, interferencia o decepción de forma intencionada de las señales electromagnéticas empleadas por los sistemas de comunicaciones, navegación, vigilancia y control aeroespacial, constituye una amenaza, cuyo impacto puede llegar a ser crítico para el funcionamiento de los servicios necesarios, no sólo en el ámbito aeroespacial, sino también en el financiero, comercial, etc.

Crimen organizado

Los tráficos ilícitos constituyen la principal actividad desarrollada por la delincuencia organizada transnacional y frecuentemente emplean medios aéreos para transportar mercancías ilegales (drogas, productos falsificados, mercancías de contrabando, armas pequeñas y ligeras, etc.) y los beneficios obtenidos en ese comercio ilícito.

El transporte aéreo es también uno de los medios principales utilizados para el tráfico ilegal de personas y la trata de seres humanos. Las conexiones aéreas de España, especialmente con Sudamérica o Asia, conforman los principales escenarios de riesgo, como destino o tránsito de dichos tráficos ilícitos.

Para las organizaciones criminales los medios aeroespaciales constituyen una opción operativa importante y de fácil acceso para realizar tráficos ilícitos. Especialmente, en distancias cortas, los medios más empleados (avionetas, ultraligeros, helicópteros y aeronaves no tripuladas) son muy difíciles de detectar, identificar y clasificar, y consecuentemente, se dificulta enormemente la capacidad de intervención.

Las organizaciones criminales pueden contar en algunas ocasiones, con la connivencia de empleados de las compañías aéreas y con la ayuda de trabajadores de las infraestructuras aeroportuarias, lo cual establece un escenario de especial vulnerabilidad.

Por su naturaleza, la actividad principal de los tráficos ilícitos y las conductas asociadas para desarrollarla (por ejemplo, la falsificación de documentos de identidad de pasajeros o mercancías, o los ciberataques de apoyo) conforman una actividad relevante

CVE: BOD-2019-086-11406
Verificable en https://sede.defensa.gob.es/acceda/bod

de riesgo por cuanto supone una vulneración de la capacidad de control preventivo en las rutas e infraestructuras aéreas

Proliferación de Armas de Destrucción Masiva

La proliferación de armas con efectos potencialmente devastadores: nucleares, radiológicas, biológicas o químicas –NRBQ–, los medios aéreos utilizados para su transporte y los vectores utilizados para su diseminación (principalmente misiles), constituyen una de las principales amenazas para cualquier nación.

La creciente facilidad de cualquier actor para poder acceder a la tecnología y a la información especializada necesaria para el desarrollo de vectores portadores y de armas de destrucción masiva, preocupa especialmente a la comunidad internacional. En la actualidad, más de treinta países disponen de misiles que pueden alcanzar objetivos situados a decenas de miles de kilómetros desde su lugar de lanzamiento, portando ojivas convencionales o de destrucción masiva (nuclear, bacteriológica, química...).

Aún más grave, la posibilidad de que este tipo de armas caigan en manos de actores no estatales, organizaciones criminales o grupos terroristas es una realidad, por lo que disponer de las capacidades necesarias para combatirlas, independientemente del medio de transporte y diseminación que pueda ser utilizado, debe ser una prioridad para la nación y para toda la comunidad internacional.

Espionaje

Una de las primeras utilizaciones de los globos aerostáticos fue el reconocimiento militar. La ventaja que proporciona el dominio de la tercera dimensión ha impulsado a lo largo de los años el desarrollo de ingenios aeroespaciales que recogen información en todas las bandas de frecuencia y las procesan en beneficio de un propósito determinado.

En los tiempos actuales, la información disponible en internet llega a todos los niveles, desde el Estado hasta el ciudadano de a pie, por lo que el espionaje utiliza cada vez más las fuentes abiertas. No obstante, la información obtenida desde ingenios aeroespaciales (aeronaves, aeronaves no tripuladas, micro-satélites, satélites) pertenecientes a Estados, organizaciones internacionales, alianzas, empresas e individuos, es mayor que nunca en la historia.

El espacio ultraterrestre es el entorno preferido para las tareas de observación y recogida de información en todo el espectro de frecuencias. Cuenta con la enorme ventaja de un alcance global, operando fuera del área de soberanía de los Estados. Los medios aeroespaciales que operan en el espacio aéreo son especialmente útiles en tiempos de conflicto por la cantidad, calidad y precisión de los datos que pueden obtener, pero no pueden utilizarse fuera de esa circunstancia sin el permiso de los Estados.

La franja intermedia del espacio aéreo no es formalmente espacio aéreo de soberanía, ya que no existe un acuerdo internacional sobre la delimitación entre el espacio aéreo y el espacio ultraterrestre, pero su utilización por otro país sin permiso del país sobrevolado sería probablemente interpretada como una violación del espacio aéreo, que podría incluso desembocar en la neutralización del ingenio.

Una parte importantísima del espionaje se realiza sobre las comunicaciones. La interceptación de comunicaciones, que transitan por el espacio aéreo y ultraterrestre, desde medios en tierra, en el aire y el espacio, representa una amenaza para la seguridad difícilmente cuantificable pero cierta. Las comunicaciones especialmente sensibles como las militares o las gubernamentales deben protegerse con medidas de protección de la transmisión y del contenido (encriptación), y el desarrollo de estas capacidades de protección es esencial y estratégica para el país.

El espionaje ha superado hace mucho tiempo el contexto tradicional y, hoy en día, cobra especial relevancia el espionaje industrial. Para realizarlo, los países y las empresas utilizan todo tipo de técnicas y por supuesto utilizan profusamente los medios aeroespaciales (aeronaves, aeronaves no tripuladas, satélites…) para obtener

CVE: BOD-2019-086-11407
Verificable en https://sede.defensa.gob.es/acceda/bod

información sensible. Las tecnologías y capacidades especiales, que puedan poseer las empresas nacionales del sector aeroespacial o de sectores relacionados, deben ser protegidas de esta amenaza.

Ciberamenazas

El sector aeroespacial está altamente tecnificado e intrínsecamente vinculado al dominio cibernético y constituye un objetivo de alto valor estratégico. Cuenta con un gran componente tecnológico de avanzados sistemas de información y telecomunicaciones, aislados o integrados en redes, que se distribuyen globalmente y dan servicio a un complejo entramado de centros de seguimiento y control, radares, comunicaciones digitales de voz y datos, aeronaves y sus sistemas a bordo, y diversas instalaciones aeroportuarias. El componente espacial de este ámbito contiene infraestructuras como estaciones de control y seguimiento de satélites, centros de operaciones para vigilancia espacial, centros de comunicaciones y de procesado de datos espaciales, con un elevadísimo grado de interconexión cibernética.

Los objetivos a alcanzar con los ciberataques en el ámbito aeroespacial son muy diversos y pueden ir desde la modificación no autorizada de la información contenida en las bases de datos de los clientes, la filtración de información sensible, la alteración del mercado del tráfico aéreo, el debilitamiento de la posición competitiva de un competidor industrial hasta los ataques disruptivos contra los sistemas de las aeronaves, los sistemas de control de tierra, las ayudas a la navegación o los sistemas de coordinación de tráfico aéreo nacional, lo que podría afectar a la seguridad de las aeronaves, del transporte aéreo y de los viajeros.

Para poder realizar ciberataques complejos en este dominio es necesario disponer de una gran cantidad de recursos que no están al alcance de todos, por lo que los atacantes más probables serían Estados extranjeros en el marco de operaciones híbridas.

La tecnología es susceptible de presentar fallos de diseño, programación o fabricación, que pueden originar graves vulnerabilidades en los componentes y sistemas aeroespaciales. Los rápidos avances en el sector tecnológico provocan que, en ocasiones, los desarrollos en componentes y sistemas estén más orientados a la seguridad operativa y funcional que a su protección frente a agresiones externas lo que origina vulnerabilidades susceptibles de ser explotadas. Para alcanzar un elevado nivel de seguridad aeroespacial es necesario alcanzar previamente la seguridad cibernética de sus sistemas componentes.

Los ciberataques en el ámbito aeroespacial son una actividad de máxima rentabilidad. Un ciberataque efectivo podría provocar la inoperatividad total o parcial del elemento o sistema atacado, o una la falta de fiabilidad por la falsedad de la información que proporcionan o contienen. Ello podría suponer desde una interrupción o deficiencia menor en un servicio no esencial, hasta la disrupción de determinados sistemas y servicios críticos para la nación. De esta realidad resulta la imprescindible protección de los medios y servicios del sector aeroespacial contra ciberataques.

Desafíos

Emergencias y catástrofes

Tal y como establece la actual Estrategia de Seguridad Nacional, las emergencias y catástrofes siguen siendo uno de los principales desafíos del mundo moderno. Su impacto no sólo afecta a la vida y salud de las personas sino, también, a los bienes patrimoniales, al medio ambiente y al desarrollo económico.

En el ámbito aeroespacial las emergencias y catástrofes pueden afectar de forma muy importante al normal desarrollo de las actividades.

CVE: BOD-2019-086-11408
Verificable en https://sede.defensa.gob.es/acceda/bod

Los desafíos principales procedentes del medio natural espacial son:

– Las alteraciones causadas por la denominada «meteorología espacial» debidas a la actividad solar (tormentas, eyecciones coronales de masa, viento solar, emisión de partículas y radiación), a la radiación cósmica, y a las partículas de alta energía provenientes del espacio interestelar, provocan cambios en la magnetosfera terrestre, ionización de las capas altas de la atmósfera y tormentas geomagnéticas, cuyas consecuencias más adversas son el bloqueo de radiocomunicaciones, los daños de componentes electrónicos de satélites y en redes de transmisión de electricidad, la degradación de señales de sistemas satelitales de navegación y los daños por radiación a tripulantes de vehículos aeroespaciales. Los eventos extremos de meteorología espacial son raros (estadísticamente se producen cada 100 o 200 años), pero tienen un potencial catastrófico.

– La entrada en la atmósfera terrestre de asteroides y cometas. Se estima que orbitan el sol, cerca de la Tierra, casi 10.000.000.000 (10^{10}) de estos objetos mayores de un 1 m y más de 10.000.000 (10^{7}) mayores de 20 m. La probabilidad de entrada de objetos mayores de 10 m es de 1 cada 5 años; estos objetos pueden provocar daños en edificios y heridas en personas (como el evento de Chelyabinsk, Rusia, en 2013).

Los desafíos principales procedentes de objetos espaciales artificiales (basura espacial, vehículos espaciales, satélites) son:

– La colisión de estos objetos entre sí.
– Sus explosiones o fragmentaciones.
– Su entrada descontrolada en la atmósfera.

Se estima que hay más de 750.000 objetos de más de 1 cm de tamaño que orbitan la Tierra, con potencial destructivo en caso de colisión con objetos activos. Al año entran en la atmósfera de forma descontrolada unas 100 toneladas de objetos, a un ritmo de 1 evento de tamaño medio-alto por semana. El problema es creciente debido al aumento de lanzamientos de objetos al espacio (mega constelaciones de pequeños satélites y pequeños lanzadores), al abaratamiento del acceso al espacio y la consecuente entrada de nuevos países y actores en la carrera espacial, y al denominado efecto Kessler de multiplicación de basura espacial por la colisión en cascada.

Los desafíos principales procedentes de la atmósfera son:

– La meteorología atmosférica que puede afectar a la calidad de los enlaces de transmisión y recepción de datos de satélites, así como a la toma de imágenes ópticas desde satélite. Los fenómenos meteorológicos adversos disminuyen la seguridad de las operaciones aéreas, condicionando las rutas de vuelo y los aeropuertos usados como alternativos.

– Las erupciones volcánicas ya han demostrado el alto poder disruptivo al transporte aéreo. En 2010 la erupción en Islandia del volcán Eyjafjallajökull, provocó cancelaciones y desvíos masivos en toda Europa. Las cenizas volcánicas originadas por las erupciones volcánicas pueden formar nubes que representan un riesgo para el vuelo; suelen permanecer un tiempo considerable en la atmósfera, pudiendo originar graves consecuencias ambientales y económicas.

– El cambio climático (entendido como cambio en la distribución estadística de los patrones meteorológicos en un periodo de tiempo prolongado) puede incrementar el número de fenómenos meteorológicos extremos y adversos con consecuencias disruptivas para la aviación.

Las catástrofes aeronáuticas, accidentes o desastres provocados, tienen un gran impacto mediático en la sociedad, generan desconfianza en el sector y alarma social.

Asimismo, las emergencias aeronáuticas pueden convertirse en catástrofes si no pueden ser atendidas eficazmente por los organismos encargados de ejecutar los planes de reacción y los de protección civil, la búsqueda y localización de aeronaves

CVE: BOD-2019-086-11409
Verificable en https://sede.defensa.gob.es/acceda/bod

siniestradas, la notificación de accidentes e incidentes, y la asistencia a víctimas y familiares.

Epidemias y pandemias

El transporte aéreo ha posibilitado los intercambios entre sociedades como nunca antes en la historia de la humanidad. Esta facilidad constituye, en sí misma, un riesgo para la propagación de epidemias y pandemias, ya sea de forma fortuita o premeditada, pues en muchos casos no es posible detectar a sus portadores con carácter previo a la realización del vuelo ni durante el mismo. El ébola, o el zika, son solo algunos ejemplos de virus que potencialmente podrían propagarse en medios de transporte aéreo si no se articulan los mecanismos de prevención adecuados.

Los productos de origen animal frescos, madurados o curados, aerotransportados desde zonas afectadas por enfermedades contagiosas para el ganado, son capaces de portar patógenos viables, sirviendo de fuente de infección para otros animales. La fiebre aftosa y la peste porcina son algunos ejemplos.

De igual modo, los productos vegetales pueden traer plagas o enfermedades muy peligrosas para bosques y cultivos.

En los últimos años se está produciendo un incremento en el tráfico de animales (aves y reptiles entre otros) transportados en equipajes adaptados para el transporte por el pasajero, sin ningún tipo de control sanitario. Además, existe el riesgo de importación oculta en los equipajes de especies catalogadas en la normativa nacional como exóticas invasoras, que podrían acabar aniquilando especies autóctonas.

Por último, las aeronaves en sí mismas pueden ser un medio de propagación de determinadas especies de insectos, como los mosquitos, que pueden provocar epidemias o plagas si no se toman las medidas de desinsectación apropiadas. Por ejemplo, los insectos son los agentes transmisores de la «Xylella fastidiosa», una plaga que ataca a diversas plantas como la vid, el olivo, el almendro, el ciruelo, el melocotón, el limonero y el laurel, sin que se haya encontrado un remedio.

Contaminación atmosférica y acústica

Un factor clave para la seguridad aeroespacial nacional es la compatibilización de las operaciones aéreas con el entorno, impulsando medidas que lleven a la disminución de ruidos y afecciones en el medio natural, así como a la reducción de las emisiones contaminantes.

Con el crecimiento previsto del tráfico aéreo para las próximas décadas, los problemas medioambientales asociados a la operación de las aeronaves podrían suponer una limitación significativa al desarrollo económico en determinadas ciudades o regiones.

Los sistemas espaciales apenas tienen impacto en la contaminación atmosférica con la excepción de los vehículos lanzadores y la vaporización o caída de objetos que hacen su reentrada en la atmósfera y que pueden contener sustancias tóxicas (como la hidracina). Con respecto a la contaminación acústica, el único impacto es el de los lanzadores, que afecta muy levemente a la población, debido a las localizaciones remotas de las bases de lanzamiento, la corta duración de los lanzamientos y su baja frecuencia.

CAPÍTULO 3

Objetivo, principios y líneas de acción

Objetivo. Los principios rectores

La Estrategia de Seguridad Nacional de 2017 define para el ámbito aeroespacial el objetivo de «Garantizar la seguridad del espacio aéreo y ultraterrestre en un marco

CVE: BOD-2019-086-11410
Verificable en https://sede.defensa.gob.es/acceda/bod

compartido y orientado a prevenir las amenazas y desafíos que en ellos se desarrollan, así como a neutralizar sus consecuencias, conforme a los principios de eficiencia y máxima coordinación, tanto en el empleo de las capacidades de análisis y evaluación como en las de respuesta ante los desafíos».

Las distintas administraciones que configuran el Estado cuentan con una sólida estructura permanente que, debidamente coordinada, debe proporcionar a la sociedad un adecuado nivel de protección ante las amenazas previamente descritas, que evolucionan con la velocidad de los cambios tecnológicos.

Dado que el ámbito aeroespacial es un entramado complejo en el que participan muchos países, asegurar la coordinación exterior con nuestros aliados mediante consultas bilaterales y multilaterales, entre otros medios, es vital para alcanzar la mayor eficiencia y resiliencia de nuestro sistema de seguridad aeroespacial cuya coordinación interna es condición indispensable e inexcusable para alcanzar un alto grado de coordinación externa.

Los principios rectores definidos en la Estrategia de Seguridad Nacional 2017: unidad de acción, anticipación, eficiencia y resiliencia, son plenamente aplicables en el ámbito de la seguridad aeroespacial.

Unidad de Acción: Toda respuesta ante una incidencia en el ámbito de la seguridad aeroespacial que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

Para conseguirla es necesario disponer de personal especializado con una preparación adecuada, que se alcanza mediante el entrenamiento, y la difusión de información entre los organismos implicados.

Una gestión centralizada de las crisis que afecten al ámbito aeroespacial, permite mantener una visión completa de la situación de la amenaza o desafío, y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

Anticipación: La especificidad del medio aeroespacial y de los actores implicados, demanda que existan mecanismos de anticipación en organismos especializados, que proporcionen la inteligencia aeroespacial necesaria para orientar la acción del Estado en situaciones de crisis.

La anticipación prima las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, que compartan información en tiempo casi real, permite disponer de un adecuado conocimiento de la situación aeroespacial. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas y desafíos.

Eficiencia: La seguridad aeroespacial precisa del empleo de sistemas multipropósito de alto nivel tecnológico, que llevan asociados unas necesidades muy exigentes de operación y sostenimiento. Estos sistemas son en general muy complejos, requieren una planificación anticipada, y tienen un elevado coste derivado de su desarrollo, adquisición, operación y sostenimiento.

El escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción aeroespacial del Estado hacia la optimización de los recursos dedicados a la seguridad aeroespacial. Unidad de acción, compartición de información e integración de recursos resultarán indispensables para alcanzar la eficiencia deseada.

Resiliencia: La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas del ámbito aeroespacial. Tratándose de un sector clave y un capacitador de la actividad del resto de ámbitos, es previsible que se vea amenazado desde los primeros estadios de cualquier crisis.

El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra amenazas y desafíos. Especial mención merece el refuerzo que requieren, frente a las ciberamenazas o la perturbación electrónica, las redes de información y comunicaciones, y los sistemas de mando y control, elementos imprescindibles en el ámbito aeroespacial.

CVE: BOD-2019-086-11411
Verificable en https://sede.defensa.gob.es/acceda/bod

Líneas de acción y medidas concretas

Del objetivo genérico definido por la Estrategia de Seguridad Nacional 2017, se derivan cinco líneas de acción que se desarrollan mediante una serie de medidas concretas para preservar la seguridad nacional en el ámbito aeroespacial.

Línea de acción 1. Fomentar una actuación coordinada de todas las Administraciones Públicas y departamentos con competencias en el espacio aéreo y ultraterrestre que permita establecer sinergias y abordar soluciones transversales

Ante la presencia de una amenaza o desafío para la seguridad y, con el conocimiento de la situación aeroespacial, debe iniciarse un proceso de orientación y evaluación de las posibles opciones de respuesta. La necesidad de minimizar el posible impacto exige la existencia de unas estructuras y protocolos que minimicen el tiempo de reacción y agilicen la respuesta. Dichos mecanismos deben fortalecer los lazos transversales en la Administración, favoreciendo la delegación de competencias y la descentralización en la ejecución de acciones.

Dado el alto coste, en recursos y en tiempo, de la adquisición de capacidades aeroespaciales, es esencial evitar duplicidades entre los distintos departamentos mediante un adecuado reparto de responsabilidades y medios. La designación de organismos proveedores de determinados servicios de forma centralizada para todo el Estado, en función de su mejor adecuación, experiencia o disponibilidad, redundará en la mejora del rendimiento global de los recursos. Este modelo estaría enfocado a alcanzar la unidad de acción aeroespacial del Estado, alineando sus esfuerzos para ser más sostenibles y más eficientes.

Las medidas que desarrollan está línea de acción, hacen hincapié en cuatro áreas principales: Coordinación, Estructuras, Formación y Cultura de Seguridad.

Coordinación:

Mejorar y desarrollar la acción coordinada y el intercambio de información relevante entre los distintos niveles de la administración pública y con los elementos de la sociedad civil que se consideren necesarios, de forma que las autoridades designadas dispongan de la información necesaria y en tiempo útil para la toma de decisiones en situaciones de crisis.

Específicamente:

– Reforzar los mecanismos de coordinación y fomentar sinergias entre las distintas administraciones y organismos involucradas en la seguridad aeroespacial.

– Hacer uso de todas las fuentes de información disponibles, incluyendo el «big data», la inteligencia artificial y la simulación de efectos de respuesta, para anticipar, en lo posible, las situaciones de crisis que puedan presentarse en el ámbito aeroespacial y preparar las respuestas adecuadas.

– Impulsar la cooperación en materia de inteligencia e investigación criminal sobre los riesgos que amenazan al sector aeroespacial.

– Impulsar la acción coordinada de los organismos estatales ante las amenazas y desafíos, estableciendo protocolos de actuación y desarrollando las capacidades necesarias.

– Mejorar la coordinación e intercambio de información entre las distintas agencias y organismos que tienen responsabilidades en la regulación, producción, gestión, control y operación de aeronaves no tripuladas.

– Establecer entre las distintas administraciones los planes de prevención y de respuesta encaminados a hacer frente al desafío de pandemias y epidemias que se puedan transmitir mediante el empleo del transporte aéreo.

– Incrementar la eficiencia explotando las sinergias en capacidades aeroespaciales entre organizaciones dependientes de la administración, así como las colaboraciones

CVE: BOD-2019-086-11412
Verificable en https://sede.defensa.gob.es/acceda/bod

con la empresa privada, promoviendo la optimización y distribución de los recursos de la forma más eficiente para un mejor aprovechamiento del gasto público.

Estructuras:

En el ámbito aeroespacial resulta crucial desarrollar y mantener una capacidad de respuesta suficientemente ágil y adecuada ante aquellos eventos que puedan afectar a la Seguridad Nacional. Dicha capacidad requiere de cuatro elementos esenciales:

– Un sistema unificado de observación, vigilancia y control permanentes que permita conocer en tiempo casi real la situación aeroespacial y sus posibles amenazas.
– Un sistema que aporte visibilidad integral sobre los medios de respuesta disponibles para llevar a cabo la acción correctora elegida.
– Una estructura de decisión centralizada y ágil, basada en un marco regulador que favorezca la transversalidad y la descentralización de la ejecución.
– Un componente humano experto que, empleando su formación, experiencia y la información disponible, sea capaz de orientar adecuadamente la situación y proponer opciones de respuesta.

Formación y adiestramiento:

– Mejorar aquellos aspectos relacionados con la formación y el adiestramiento avanzado en la actuación coordinada contra los diferentes escenarios de crisis, catástrofes y degradación de los sistemas asociados al ámbito aeroespacial.
– Realizar regularmente ejercicios de gestión de crisis interministeriales e internacionales, para preparar el sistema de gestión de crisis en diferentes escenarios y evaluar su respuesta, resistencia y resiliencia.

Cultura de seguridad:

– Mejorar la cultura de seguridad aeroespacial en todos los ámbitos relevantes de la Administración Pública mediante reuniones periódicas de coordinación, jornadas divulgativas en materia de seguridad, seminarios específicos, etc.
– Fomentar y divulgar la cultura de seguridad aeroespacial a todos los niveles de la sociedad mediante una política de información y comunicación social transparente, activa y participativa.
– Aprovechar las tecnologías que permiten la compartición e interacción de información, de forma que la comunicación de las medidas de prevención y/o de las consecuencias de los riesgos y amenazas se haga de forma veraz, ágil, coherente y coordinada.

Línea de acción 2. Fortalecer las capacidades de los organismos e instituciones nacionales, tanto públicos como privados, con competencias en estos ámbitos, para hacer frente a las diversas amenazas y desafíos propios del espacio aéreo y ultraterrestre

Las medidas para el fortalecimiento de las capacidades nacionales en el sector aeroespacial pueden clasificarse en dos grandes apartados, medidas de tipo legal y, medidas de incremento y mejora de las capacidades. Las primeras buscan establecer un marco legal claro que regule las actividades en el espacio aéreo y ultraterrestre, mientras que las segundas buscan el incremento y mejora de capacidades que permita hacer efectiva la seguridad aeroespacial.

Medidas legales:

– Seguir impulsando la regulación nacional e internacional del espacio ultraterrestre.
– Dada la indefinición existente sobre el límite superior de la soberanía del espacio aéreo nacional y la previsible proliferación de ingenios aéreos que operarán por encima

CVE: BOD-2019-086-11413
Verificable en https://sede.defensa.gob.es/acceda/bod

del espacio aéreo controlado, impulsar la regulación del espacio aéreo comprendido entre el actual espacio aéreo controlado y el espacio ultraterrestre, considerando las iniciativas internacionales y europeas en la materia.

– Actualizar el código penal y la Ley Penal y Procesal de la Navegación Aérea (1964) para tipificar delitos en el ámbito aeroespacial, relacionados con la violación de las normas que regulan el empleo de los espacios aéreo y ultraterrestre, y que supongan una grave amenaza para los medios e infraestructuras aeroespaciales y consecuentemente, para la seguridad de los ciudadanos.

Medidas de incremento y mejora de las capacidades:

– Reforzar constantemente los sistemas nacionales, civil y militar, de vigilancia y control del espacio aéreo, para que incorporen información transversal de otros organismos, de forma que se incrementen sus capacidades de detección, identificación y clasificación, y su eficacia y resiliencia ante las amenazas y desafíos en el ámbito aeroespacial.

– Impulsar el desarrollo de una capacidad nacional dual de vigilancia y seguimiento del espacio ultraterrestre, íntimamente interconectada e integrada con las capacidades de vigilancia, seguimiento y control del espacio aéreo.

– Incrementar y mejorar las capacidades necesarias para hacer frente al empleo de plataformas aéreas en acciones contra la seguridad nacional, e impulsar la colaboración y coordinación entre el sistema nacional de vigilancia y control del espacio aéreo, las fuerzas y cuerpos de seguridad del Estado, y los entes autonómicos y locales, difundiendo y armonizando los procedimientos relativos a la detección de posibles comportamientos delictivos en este tipo de plataformas.

– Desarrollar la capacidad de inteligencia espacial y la protección de los medios espaciales, para mantener nuestros servicios espaciales esenciales protegidos contra acciones de perturbación, guerra electrónica y destrucción, inhabilitación o neutralización.

– Incrementar la capacidad de supervivencia de infraestructuras críticas aeroespaciales, en particular los sistemas de vigilancia, control y defensa aeroespaciales, y las redes de información y comunicaciones aeroespaciales, mediante la protección física y cibernética, el servicio de alerta de colisiones de satélites, y la disposición de redundancias que aumenten su resiliencia y garanticen su supervivencia en caso de la materialización de una amenaza, un fallo grave o una degradación sobrevenida.

– Fortalecer y consolidar de forma colaborativa la base industrial nacional del sector aeroespacial, impulsando las capacidades tecnológicas e industriales propias y la participación en programas internacionales, tanto a nivel bilateral, multilateral o derivados de nuestra pertenencia a organizaciones como la Unión Europea y la OTAN, que permitan adquirir conocimiento y experiencia, obtener sinergias, compartir y aumentar el espectro de colaboración, así como reducir la inversión para la adquisición de dichas capacidades.

– Fortalecer la industria aeroespacial nacional para obtener una mayor autonomía y soberanía, reduciendo la dependencia de terceros países.

– Fomentar las sinergias de las actividades y tecnologías duales.

– Impulsar la dimensión de seguridad en la innovación, la investigación básica y el desarrollo tecnológico.

– Detectar amenazas y desafíos aeroespaciales mediante el desarrollo de nuevas herramientas que utilicen los avances tecnológicos en inteligencia artificial, «big data», etc.

– Impulsar e implantar tecnologías avanzadas en el proceso de identificación de los viajeros que transitan por nuestros aeropuertos. Establecer bases de datos armonizables nacional e internacionalmente.

CVE: BOD-2019-086-11414
Verificable en https://sede.defensa.gob.es/acceda/bod

– Activar los protocolos de actuación contra las pandemias liderados por las organizaciones competentes (principalmente OMS) y su coordinación con los protocolos nacionales.

– Establecer y evaluar los protocolos nacionales contra pandemias.

– Completar e incorporar medidas de protección medioambiental en el ámbito aeroespacial.

Línea de acción 3. Perseverar en el análisis de riesgos y evaluación de medidas contra ciberataques, actos terroristas o delictivos u otros conflictos que afecten a las instalaciones aeroportuarias o al transporte aéreo, dentro o fuera del espacio aéreo español

Ciberamenazas:

Las características más preocupantes de las ciberamenazas son su impacto transversal, su globalidad por la ausencia de fronteras geográficas, su fácil expansión y propagación debido a la interconectividad, la dificultad en su detección, y la impunidad derivada de una compleja atribución. Por ello, es necesario afrontar esta amenaza al sector aeroespacial con medidas de fortalecimiento interno, inteligencia, cooperación internacional, y normativa y legislación.

– Fortalecer las capacidades de prevención, detección, vigilancia y respuesta a los ciberataques, impulsando los planes contemplados en la Estrategia de Ciberseguridad Nacional y dotándolos de los recursos necesarios.

– Adecuación de los sistemas informáticos y operativos al Esquema Nacional de Seguridad (ENS) en las Administraciones Públicas del ámbito aeroespacial.

– Fomentar el empleo de soluciones, productos, sistemas y servicios confiables, certificados en entornos y equipos acreditados en redes sensibles.

– Concienciar en ciberseguridad a los principales actores nacionales del sector aeroespacial, adoptando procedimientos y buenas prácticas como las relativas a las actualizaciones de seguridad de los sistemas.

– Incorporar la Inteligencia sobre las ciberamenazas, para aportar un valor predictivo y estratégico, como complemento indispensable a las medidas de seguridad físicas y lógicas.

– Utilizar medidas de contrainteligencia para ayudar a contrarrestar las ciberamenazas en el ámbito aeroespacial.

– Fomentar la cooperación con otros estados y organizaciones internacionales para establecer un marco estratégico internacional de estabilidad cíber en el ámbito de la seguridad aeroespacial que posibilite la cooperación estratégica (creación de capacidades defensivas, intercambio de buenas prácticas, fomento de la presencia internacional, etc.) y la táctica (intercambio entre Equipos de Respuesta a Incidentes de Seguridad de la Información (CERT), formación de expertos, etc.).

– Impulsar el desarrollo de la legislación internacional específica cíber para establecer un marco legislativo común, como la Directiva europea de Seguridad de las Redes y Sistemas de Información –NIS- traspuesta a la legislación nacional por el RDL 12/2018.

– Implantar una política integral de ciberseguridad en el ámbito aeroespacial acorde a los principios establecidos en la Estrategia de Ciberseguridad Nacional, que:

• promueva arquitecturas de sistemas redundantes, resistentes y resilientes a agresiones cibernéticas;
• gestione la obsolescencia de los sistemas aeroespaciales;
• audite la ciberseguridad de los sistemas más críticos;
• determine la formación específica en ciberseguridad del personal que opera y sostiene sistemas aeroespaciales;
• organice ejercicios para evaluar los sistemas y el personal.

CVE: BOD-2019-086-11415
Verificable en https://sede.defensa.gob.es/acceda/bod

– Incorporar criterios de ciberseguridad tanto en los documentos de definición de requisitos y de viabilidad de los procesos de obtención de capacidades aeroespaciales, como en las actividades de sostenimiento que se realizan a plataformas e instalaciones críticas vinculadas al sector.

Terrorismo:

En la lucha contra el terrorismo, el intercambio ágil de información es un elemento esencial para afrontar la amenaza a la que se enfrenta el sector aeroespacial por parte de las organizaciones terroristas. La gran capacidad de adaptación de estos grupos a las medidas de todo tipo que se adopten, exige de la existencia de unos canales específicos de distribución de inteligencia sobre:

– amenazas específicas al sector aeroespacial, en el interior y el exterior de España;
– tácticas, técnicas y procedimientos que estén desarrollando los grupos terroristas para soslayar las medidas de seguridad implementadas.

Como complemento a las medidas anteriores, es indispensable incrementar la seguridad del personal que trabaja u opera en las instalaciones aeroportuarias e infraestructuras críticas asociadas al transporte aéreo mediante:

– la determinación del nivel de clasificación de seguridad necesario para acceder a las áreas sensibles de dichas instalaciones e infraestructuras;
– el impulso al desarrollo de la legislación pertinente y la determinación del procedimiento de obtención de la habilitación.

Amenazas emergentes:

– Mantener un adecuado nivel de inteligencia sobre el estado de los desarrollos tecnológicos emergentes que puedan ser empleados contra las capacidades aeroespaciales de la nación.

Desafíos:

– Desarrollar e implementar el conjunto de medidas técnicas, de continuidad de operaciones y de recuperación de desastres, en el marco de los planes sectoriales del ámbito de la Protección de la Infraestructuras Críticas (PIC), tanto para el subsector de transporte aéreo como para el sector espacio.
– Incrementar las capacidades del Sistema Español de Vigilancia y Seguimiento Espacial, en coordinación con las actividades realizadas en el marco de la Agencia Espacial Europea, la Unión Europea, y otros departamentos de la Administración Pública, para incluir mejoras y nuevas funcionalidades en el área de análisis de riesgos y evaluación de medidas de seguridad, específicamente en:

• Las capacidades de detección de objetos espaciales;
• Las capacidades de procesado, incluyendo catalogación y capacidades específicas para las necesidades de seguridad espacial
• Las capacidades de provisión de servicios de vigilancia y seguimiento espacial para que puedan discriminarse los objetos catalogados e identificados como «actividad legal y registrada», de otros que puedan tener algún tipo de actividad o intención potencialmente hostiles.
• Las capacidades de análisis ante los desafíos de la meteorología espacial, los asteroides y los cometas.
• La coordinación y el intercambio de información con otros centros o servicios espaciales de seguridad (comunicaciones seguras, navegación segura, teledetección para seguridad).
• La inclusión de nuevas capacidades de análisis ante las amenazas identificadas para los casos de conflictos armados, terrorismo, crimen organizado y espionaje.

CVE: BOD-2019-086-11416
Verificable en https://sede.defensa.gob.es/acceda/bod

– Participar internacionalmente en la monitorización de la meteorología atmosférica y espacial e incorporar medidas de protección medioambiental en el ámbito aeroespacial.

Línea de acción 4. Impulsar un desarrollo normativo del uso civil de aeronaves pilotadas remotamente que garantice el necesario equilibrio entre la seguridad de las personas, instalaciones y demás usuarios del espacio aéreo, y el desarrollo tecnológico y económico de un sector pujante de la economía española

El sector de las aeronaves no tripuladas de uso civil tiene un enorme potencial, tanto por los innumerables usos que pueden tener como por el previsto peso económico que generará su actividad. Para liberar ese potencial, es condición indispensable regular los múltiples aspectos que implica su operación, y esta regulación se vuelve compleja cuando hay que hacerla compatible con otras regulaciones que ocupan el mismo espacio.

En algunos aspectos, las aeronaves no tripuladas pueden ser tratadas como las tripuladas y puede reutilizarse la normativa aeronáutica, particularizada para estas aeronaves. En este sentido se enmarcan:

– el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil, que establece y mantiene el nivel de seguridad que debe cumplir la aviación civil en la Unión Europea en la que se incluye a las aeronaves no tripuladas.

– el RD 1036/2017, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto en el espacio de soberanía aérea nacional. Se aplica principalmente a aeronaves civiles con un peso máximo al despegue menor de 150 Kg. para la realización de trabajos técnicos o científicos (operaciones aéreas especializadas en términos de la UE). La norma fija todas las condiciones que deben cumplirse para autorizar estos trabajos técnicos.

El desarrollo normativo tiene forzosamente que ir ligado al concepto de operación de las aeronaves no tripuladas. Por ejemplo, si se desea operar dentro de la circulación aérea general, tendrán que cumplir las mismas normas aplicables a las aeronaves tripuladas y con todas las garantías adicionales que exija el legislador; si el concepto de operación incluye operar múltiples aeronaves no tripuladas a baja altitud y dentro de un área urbana (concepto U-Space de la UE), la gestión del tráfico y la regulación serán muchísimo más complejas.

El desarrollo del sector debe contemplar medidas ante la utilización irresponsable, ilícita o con fines terroristas de las aeronaves no tripuladas. Concretamente será necesario:

– Impulsar los desarrollos normativos que permitan un mejor control, localización y registro de las aeronaves no tripuladas.

– Desarrollar capacidades contra aeronaves no tripuladas y la normativa que regule su uso.

– Promover la creación de centros de vigilancia, coordinación y control efectivo para aeronaves no tripuladas, principalmente en los espacios incluidos en el concepto U-Space, y establecer las normas de coordinación entre estos y los organismos del sistema nacional de vigilancia y control del espacio aéreo.

– Coordinar y gestionar los aspectos de seguridad en el marco del sistema de vigilancia y control del espacio aéreo, regulando el ámbito de actuación de cada uno de los organismos estatales con responsabilidades en el área de seguridad.

– Promover actuaciones de concienciación y sensibilización sobre el empleo de aeronaves no tripuladas por particulares.

– Desarrollar medidas legales punitivas específicas para el sector de las aeronaves no tripuladas.

CVE: BOD-2019-086-11417
Verificable en https://sede.defensa.gob.es/acceda/bod

Línea de acción 5. Apoyar el papel de España en el ámbito internacional, dentro del marco de compromisos y responsabilidades asumidos en materia de seguridad aérea y ultraterrestre

España tradicionalmente participa en múltiples programas, foros, comités y grupos de trabajo de organizaciones internacionales civiles y militares del ámbito aeroespacial. Su sistema de defensa aéreo está al nivel de los mejores de Europa y está interconectado e integrado en el de la Alianza Atlántica; igualmente, su sistema de control aéreo civil es uno de los mayores y más complejos de Europa y está interconectado con EUROCONTROL. En los últimos años se está desarrollando el Sistema Español de Vigilancia y Seguimiento Espacial, como colaboración nacional al programa de la regulación actual Espacial de la Unión Europea, para extender la vigilancia y el seguimiento sobre las amenazas y desafíos provenientes del espacio ultraterrestre.

La Alianza Atlántica reconoce que las capacidades basadas en el espacio son imprescindibles para el mando y control de las operaciones y como apoyo en la toma de decisiones, por lo que es esencial en la política defensiva y de disuasión. La cumbre de Jefes de Estado y de Gobierno de Bruselas, julio 2018, acordó desarrollar la «Política Espacial de la Alianza».

Las medidas para potenciar el ámbito aeroespacial en materia de seguridad incluyen:

– Fomentar la inversión, participación activa y representación de España en todas las organizaciones, comités, programas, foros, iniciativas y grupos de trabajo internacionales en materia de seguridad aeroespacial de interés.

– Suscribir acuerdos de seguridad aeroespacial bilaterales, fundamentalmente con los países limítrofes, y multilaterales, preferentemente con los países europeos más influyentes y las potencias espaciales globales, para apoyo mutuo en situaciones de crisis.

– Potenciar la cooperación policial internacional en la investigación criminal de temas aeroespaciales de su competencia para amenazas de crimen organizado, terrorismo y cíber.

– Potenciar los mecanismos de intercambio de información de vigilancia espacial con los centros y organismos (civiles y militares) de otras naciones cuya cobertura complementa y completa la de nuestro sistema de vigilancia espacial.

– Asegurar la interoperabilidad con los sistemas de mando y control aeroespaciales de los países de la OTAN/UE, para el correcto desempeño de las funciones de seguridad y defensa en el espacio aéreo de soberanía, responsabilidad o interés nacional.

– Utilizar los mecanismos de financiación comunitarios para fortalecer, consolidar y mejorar la base industrial aeroespacial, contribuyendo a la economía y seguridad de la nación.

– Potenciar el desarrollo nacional e internacional de las capacidades espaciales de doble uso.

– Mejorar la capacidad de previsión meteorológica y contribuir en el desarrollo de protocolos internacionales de prevención, alerta y actuación en caso de fenómenos meteorológicos adversos, inclusive los de origen ultraterrestre, en línea con los estudios y planes de protección establecidos para los fenómenos de Meteorología Espacial.

– Cooperar internacionalmente para paliar los efectos nocivos de la aviación mediante la mejora de la eficiencia energética, el uso de energías renovables y biocombustibles, y la disminución del ruido en los entornos aeroportuarios.

– Impulsar la coordinación internacional para la prevención y control de la propagación de enfermedades contagiosas a través del sistema de transporte aéreo internacional.

CVE: BOD-2019-086-11418
Verificable en https://sede.defensa.gob.es/acceda/bod

CAPÍTULO 4

La Seguridad Aeroespacial en el Sistema de Seguridad Nacional

La visión integral de la seguridad aeroespacial plasmada en esta estrategia, los riesgos y amenazas detectados que le afectan, los objetivos y líneas de acción trazados para dar una respuesta conjunta y adecuada a la preservación de la seguridad aeroespacial bajo los principios que sustentan el Sistema de Seguridad Nacional, determinan la necesidad de contar con una estructura orgánica precisa a estos efectos, que estará constituida por los siguientes componentes, bajo la dirección del Presidente del Gobierno:

A. El Consejo de Seguridad Nacional.
B. El Consejo Nacional de Seguridad Aeroespacial.
C. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.

Organización de la Seguridad Aeroespacial

A. El Consejo de Seguridad Nacional

El Consejo de Seguridad Nacional, configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

B. El Consejo Nacional de Seguridad Aeroespacial

El Consejo Nacional de Seguridad Aeroespacial dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la seguridad aeroespacial.

Funciones del Consejo Nacional de Seguridad Aeroespacial:

– Apoyar a la toma de decisiones del Consejo de Seguridad Nacional en materia de seguridad aeroespacial mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
– Apoyar al Consejo de Seguridad Nacional en materias de planificación y coordinación de la política de Seguridad Nacional relacionadas con la seguridad aeroespacial.
– Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias relacionadas con el ámbito de la seguridad aeroespacial, así como entre los sectores público y privado.
– Contribuir a la elaboración de propuestas normativas en materia de seguridad aeroespacial para su consideración por el Consejo de Seguridad Nacional.
– Evaluar el grado de desarrollo y cumplimiento de la Estrategia de Seguridad Aeroespacial Nacional e informar al Consejo de Seguridad Nacional.
– Impulsar los estudios necesarios y hacer propuestas para que la Estrategia de Seguridad Aeroespacial Nacional evolucione armónicamente con respecto a la normativa aeroespacial nacional e internacional, y a otras estrategias con dimensión internacional.
– En el ámbito de la seguridad aeroespacial: valorar los riesgos asociados a las amenazas y desafíos; analizar posibles escenarios de crisis y su evolución; elaborar y mantener actualizados los planes de respuesta; formular directrices, en el ámbito de la seguridad aeroespacial, para la realización de ejercicios de gestión de crisis, evaluando los resultados de su ejecución; todo ello en coordinación con los órganos y autoridades directamente competentes.

CVE: BOD-2019-086-11419
Verificable en https://sede.defensa.gob.es/acceda/bod

– Proponer la creación de comités y grupos de trabajo, permanentes o temporales, para la realización de determinadas funciones especializadas y, en su caso, aprobar su composición, incluyendo los expertos del sector público y privado necesarios.

– Aprobar y, en su caso, elevar los trabajos, estudios o informes de los comités y grupos de trabajo.

– Todas aquellas otras funciones que le encomiende el Consejo de Seguridad Nacional en el marco de la seguridad aeroespacial.

La composición del Consejo de Seguridad Nacional Aeroespacial reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de seguridad aeroespacial, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad.

En el Consejo podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

En el cumplimiento de sus funciones, el Consejo Nacional de Seguridad Aeroespacial será apoyado por el Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

C. El Comité de Situación

El Comité de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la seguridad aeroespacial que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata, coordinada y eficaz a través de un solo órgano de dirección político estratégica de la crisis.

El Comité de Situación y el Consejo Nacional de Seguridad Aeroespacial actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno.

El Comité de Situación será apoyado por el Departamento de Seguridad Nacional con el fin de garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Para el cumplimiento eficaz de sus funciones de apoyo al Comité de Situación, el Departamento de Seguridad Nacional podrá ser reforzado por personal especializado proveniente de los departamentos ministeriales u organismos competentes, los cuales conformarán la Célula de Coordinación específica en el ámbito de la seguridad aeroespacial.

Implantación:

La puesta en marcha del Consejo Nacional de Seguridad Aeroespacial y del Comité de Situación, y la armonización de su funcionamiento con los órganos existentes, se realizará paulatinamente mediante la aprobación de las disposiciones normativas necesarias y el reajuste de las vigentes, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes del Sistema de Seguridad Nacional.

(B. 86-3)

(Del *BOE* número 103, de 30-4-2019.)

CVE: BOD-2019-086-11420
Verificable en https://sede.defensa.gob.es/acceda/bod